March 1997

Cyberspace Self-Government: Town-Hall Democracy or Rediscovered Royalism?

Henry H. Perritt Jr.
IIT Chicago-Kent College of Law, hperritt@kentlaw.iit.edu

ARTICLE

CYBERSPACE SELF-GOVERNMENT: TOWN HALL DEMOCRACY OR REDISCOVERED ROYALISM? †

HENRY H. PERRITT, JR. ††

TABLE OF CONTENTS

† This article is the first of a trilogy of articles considering the relationship between the Internet and regulation. This article considers self-regulation. A second article will consider regulation of the Internet through traditional legal institutions. The third will consider use of the Internet to facilitate governance through traditional legal institutions and new international institutions following traditional institutional models.

†† Dean and Professor of Law, Chicago-Kent College of Law, Illinois Institute of Technology; member of the bar, Virginia, Pennsylvania, District of Columbia, Maryland, United States Supreme Court; J.D., 1975, Georgetown University Law Center; S.M., 1970, MIT; S.B., 1966, MIT. The author appreciates stimulating contributions from several members of the Villanova Law School faculty, particularly John Hyson, Joseph Dellapenna, and Richard Turkington, and from a continuing dialogue with David R. Johnson about governance of Cyberspace.

I. INTRODUCTION

Growing interest in the Global Information Infrastructure—the Clinton Administration's Information Superhighway—has given rise to suggestions that some or all of this "cyberspace" should be self-governing—autonomous with respect to the regular law.[1] Cyberspace, the set of electronic network communities, may be distinct enough to have its own law and legal institutions—a system of "cybergovernment." This self-governance may be more efficient for cyberspace. However, the rules and/or the adjudicatory techniques for applying the rules may need to be different from those of the surrounding community. In any event, compliance with the basic norms of the community may be higher when members of the cyberspace subcommunity participate in self-governance. Each of these criteria can be evaluated separately with respect to the three basic activities of governance: rulemaking (legislation), rule application (adjudication), and enforcement. More or less autonomy may be appropriate depending on whether one considers rulemaking, adjudication, or enforcement.

---

1. *See, e.g., White House Paper on Electronic Commerce* (released June 30, 1997) <http://www.iitf.nist.gov/eleccomm/exec_sum.htm>; *Bonn Declaration*, (visited Nov. 24, 1997) <http://www2.echo.lu/bonn/final.html>.

The emergence of new social communities in Internet newsgroups and on public electronic bulletin boards has already attracted comment.[2] Some markets are currently almost completely electronic in cyberspace,[3] and already govern themselves. In general, there are numerous communities that enjoy powers of self-government. Many instances of self-government are so commonplace as to escape notice. Virtually every citizen of a modern state is a member of multiple private organizations: bar associations, national fraternities, and non-profit organizations. All of these organizations exercise some powers of self-governance. Usually, there is little controversy over the application of special bodies of substantive law and the use of specialized institutions to resolve intra-organizational disputes pursuant to charters and bylaws of these organizations. It may seem strange that something can be law without being adopted by a legislature or a court, but it happens all the time and has for centuries.[4]

Self-government—legal autonomy—may also be appropriate for some new electronic communities, although it is extremely unlikely that self-governance will result just because some of the communications occur through new electronic channels. But, when all of the functions of a particular market or of other commercial communities are contained within electronic communications systems, the result is something like a community, whereby the participants may qualify for self-governance.[5] Nevertheless, while it is possible, and in this author's view desirable, for

---

2. *See* Reid Kanaley, *Transforming the Internet Into a World Wide Safety Net*, PHILADELPHIA INQUIRER, Jan. 17, 1995, at A1 (reporting on the Internet's role as a psychological safety net of support groups and crisis intervention techniques for thousands of people contemplating suicide and experiencing other distress); Peter H. Lewis, *Strangers, Not Their Computers, Build a Network in Time of Grief*, N.Y. TIMES, Mar. 8, 1994, at A1 (describing economic and personal support by members of computer forum for family of former member of forum killed in robbery).

3. Markets are economic electronic communities, and some satisfy important needs of their participants. Participants in some markets only have transitory attachments. Attendance at a single auction is an example. Participants in other markets have more than transitory attachment. Someone who regularly sells magazine articles to a group of competing publishers is an example. Certain information markets are almost completely electronic, typified by vendors such as WESTLAW, LEXIS, and Dialog. International financial markets relating to wholesale funds transfers and clearance of credit card transactions also are mostly electronic.

4. *See* discussion *infra* Part VI.

5. The idea of community presupposes shared interests and activities. "Community: 2. a group of people living together as a smaller social unit within a larger one, and having interests, work, etc. in common ...." WEBSTER'S NEW WORLD DICTIONARY 288 (2d ed. 1972).

net participants to make up their own rules and establish their own institutions of government, merely doing this does not necessarily assure them of an immunity or exemption from regular law.[6]

This article considers theoretical legal frameworks for autonomy of open networks, based upon models from other relatively autonomous communities. The article evaluates four possible justifications for electronic community self-governance, and considers sovereignty and contractual frameworks for self-government. The article reviews three attempts at self-governance: one in the alt.current-events.net-abuse newsgroup, another proposed by the International Ad Hoc Committee (IAHC), and a third represented by traditional proprietary services. The article evaluates the justification for such autonomy and inventories the major steps to be taken before credible exercises in self-government can

---

6. Terminology is a problem in talking about self-governance. The main problem arises with respect to what the traditional legal system should be called. This paper refers to it as the "traditional" community or legal system. The traditional system could also be thought of as the "surrounding" or "larger" community or legal system, but that suggests that an electronic community is entirely contained within one traditional legal system or community. While "traditional" does not communicate the precise relationship of potentially self-governing systems with other legal systems, it should be understood as referring to the legal system that ordinarily will govern some or all of the activities of the electronic community being discussed.

A glossary of technical terms may be useful at this point:

Open network refers to a computer network to which anyone may connect, as distinguished from a *closed network*, on which connections are limited to a predetermined group. *Proprietary networks* are instances of closed networks, on which connections are limited to those who have paid a fee. Proprietary networks sometimes use *proprietary protocols* for digital communications between the connected computers, further limiting the class that can connect. Open networks almost always use *open protocols* such as TCP/IP, which defines the Internet. *Open architecture* refers to the configuration of an open network.

A *network services provider* offers a means for connecting a computer to a network, as by providing a dial-up telephone number connected to a modem, which is, in turn, connected to the Internet. An *internet service provider* (ISP) is a type of network services provider. A network administration entity is a person or organization that undertakes to perform network support functions, such as assigning user names, domain names, IP addresses, and e-mail addresses to allow computers to connect to the network and to use its services.

A *network community* is a group of interdependent persons or entities that communicate with each other predominantly via a computer network. The means of communication include newsgroups, e-mail lists, Web pages, and markets and forums organized through the Web.

occur. Then the article briefly explores historical and contemporary models for such arrangements.

Based upon the theoretical frameworks, the justifications, and the models, the article concludes that considerable autonomy can be achieved through contractual arrangements featuring arbitration accompanied by choice of customary substantive law. However, there may be difficulties in defining community boundaries, in implementing effective enforcement mechanisms, and in avoiding antitrust problems in the electronic network context. The article identifies the major points of tangency between regular legal systems and new Internet systems of government. It evinces that an independent legal system for the Internet is most likely to exist if the countries of the world negotiate a kind of "hands-off" treaty, committing themselves to defer to private Internet governing institutions meeting certain criteria, and empowering existing multilateral institutions to play certain ministerial roles. The article concludes by observing that the cybergovernment inquiry is but a subset of a broader range of issues presented by the informal, conversational, and frequently transient nature of electronic transactions in a legal context that has traditionally stressed formality and paper records.

At least three recent law review articles have explicitly considered the possibility of self-governance for electronic communities.[7] This article has a broader scope than the preceding articles in that it considers self-governance and legal autonomy in cyberspace along with self-governance and legal autonomy for other types of private associations. This article also links the basic idea of cyberspace self-governance to recently-proposed mechanisms for private registration of Internet domain names.

II. EXAMPLES OF CYBERSPACE DISPUTES

There is nothing new about the possibility of disputes arising in digital electronic networks. Nor is there anything new about private

---

7. *See generally* William S. Byassee, *Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community*, 30 WAKE FOREST L. REV. 197 (1995) (emphasizing the importance of recognizing differences between on-line and physical interactions, and discussing that autonomous jurisdiction is a utopian solution); Henry H. Perritt, Jr., *President Clinton's National Information Infrastructure Initiative: Community Regained?*, 69 CHI.-KENT L. REV. 991 (1994) (Charles Green Lecture) [hereinafter Perritt, *Community Regained*] (exploring the role of new computer and communications technologies in undermining traditional communities and facilitating new ones); Henry H. Perritt, Jr., *Dispute Resolution in Electronic Network Communities*, 38 VILL. L. REV. 349 (1993) [hereinafter Perritt, *Dispute Resolution*].

governance of such networks, including the resolution of such disputes. Figure 1 shows three common disputes.

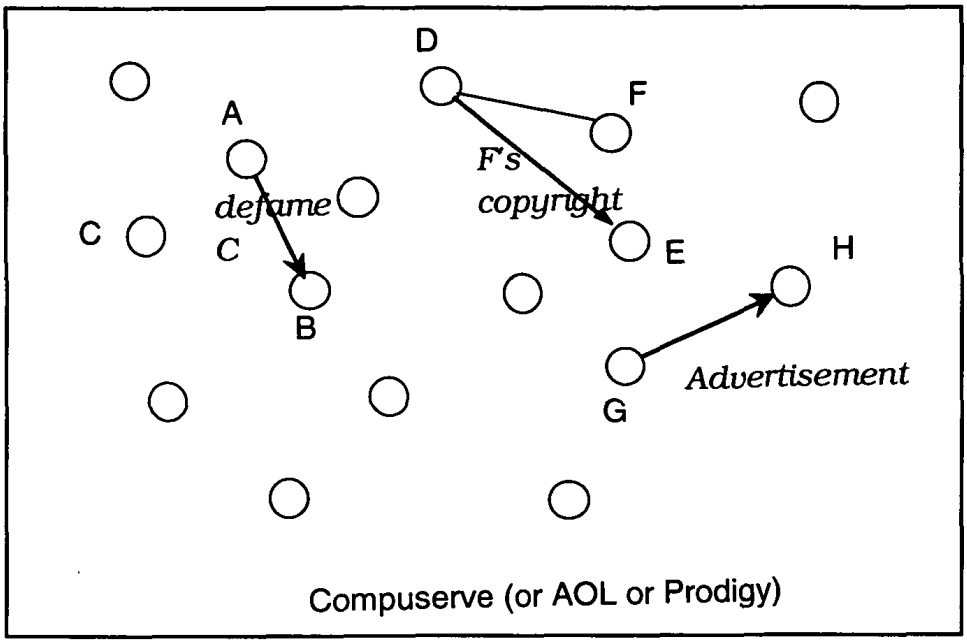

Figure 1.[8]

What is new is that a growing proportion of communications is taking place across the boundaries of proprietary network systems like CompuServe, America Online, and Prodigy, as shown in Figure 2.

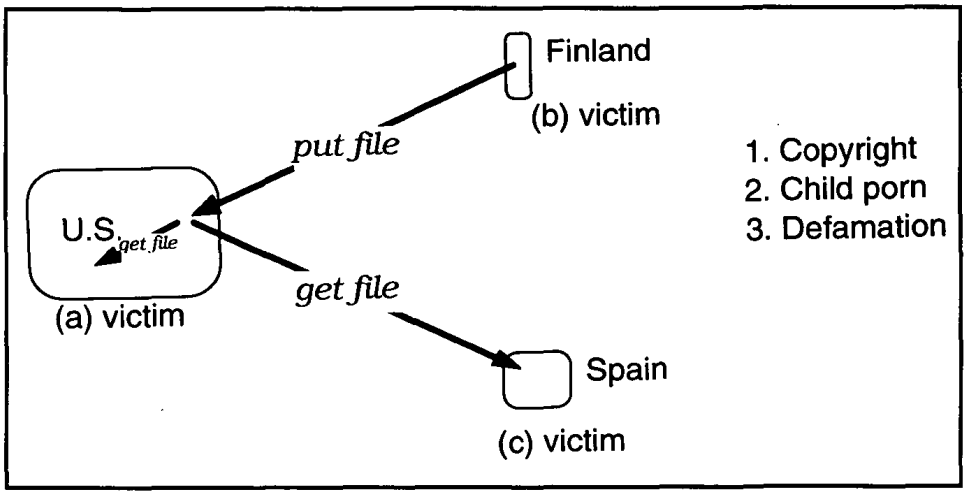

Figure 2.

8. One network user, "D," may take intellectual property belonging to another, "F," and send it to a third party, "E." One network user, "A," may defame another, "C," in a communication to "B." "G" may offend "H" by sending him an unsolicited advertisement.

A person in Finland can place a file on a computer in the United States, which can then be retrieved by someone in Spain, or in the United States. The file could infringe copyrights, contain child pornography, or be defamatory. The victim might be in the United States, in Finland, or in Spain. This means that any one network-administration entity has lost control over the activities that may give rise to controversy. In the Figure 1 scenarios, the network service provider could expel the wrongdoer. In the new open architectures, however, any one network service provider may not even know who the wrongdoer is, let alone have any control over the resource the wrongdoer wants, and the deprivation of which would represent an effective sanction.

On the one hand, the shift to open networks invites self-government, because the capacity of traditional, nationally based legal institutions to regulate the problems illustrated in Figure 1 is diminished by the transnational character of such networks. On the other hand, the capacity of the service providers—the logical organizers of regimes of self-government—is also lower in such networks because the service providers do not have the same control as they did over their own proprietary networks.

III. IS SELF-GOVERNANCE DESIRABLE?

Merely because it is conceivable that electronic communities might be self-governing, and because models for self-governance exist within recognized theoretical frameworks, does not mean that self-governance is desirable. Subcommunities within larger legal communities exercise powers of self-governance for one or more of four reasons: self-governance is more efficient; the rules and/or the adjudicatory techniques for applying the rules need to be different from those of the surrounding community; it is impracticable to apply the rules of the surrounding community; or compliance with basic norms of the community is higher when members of the subcommunity participate in self-governance. Each of these criteria can be evaluated separately with respect to the three basic activities of governance: rulemaking (legislation), rule application (adjudication), and enforcement. More or less autonomy may be appropriate depending on which of these factors one considers.[9] The following analysis of the criteria argues that self-governance is desirable for electronic communities.

---

9. The four justifications stated above are not mutually exclusive. For instance, efficiency concerns surface when one considers any of the other justifications. Moreover, the fourth justification (voluntary compliance) is a way of dealing with the third (unenforceability).

A. Self-governance may be more efficient

Self-governance may simply be a more efficient way of making and enforcing specialized rules and of enforcing rules of the larger legal system. The electronic community can enforce a norm that is supported by broad consensus in the larger society about what substantive rules ought to apply to conduct. When this occurs, it is easy for the larger legal system to defer to a self-governing community, because community institutions make exactly the same decisions that the traditional legal institutions would. It makes no real difference whether internal institutions or traditional institutions apply it; the law is the same either way.

Self-governance by electronic communities may be more efficient than governance directly through larger community mechanisms because of the inherent availability of more efficient communication technologies in electronic communities. Proposals for new rules can be published almost instantly to members of the electronic communities, and they or their representatives can debate the desirability of the proposed rules without having to assemble physically. Application of existing rules can also be more efficient using information technology because of easier detection, prompter notice, and electronic adjudication of rule violations. Indeed, an adjudicatory tribunal to hear arguments and evidence can be convened electronically. Further, the tribunal could deliberate electronically (when multiple decision-makers are involved), and make its decisions known electronically. Electronic communities may also have greater efficiency in imposing sanctions for rule violation because of the ease with which a violator can be denied access to electronic community resources.[10] A "judgment" can be executed simply by invalidating a user's password for a closed system and by removing her Internet address from routers in open systems.

B. Networks need different rules and procedures

Self-governance is desirable if different rules or adjudicatory outcomes for electronic communities are important, compared with the surrounding communities. This criterion is met when the matters addressed by self-governance are highly specialized. Specialization militates in favor of deference to the electronic community by the traditional institutions. Traditional institutions are unable, as a practical matter, to take the time to master the complexities of the specialized subject matter.

---

10. *But see infra* Part VII.A.3 (describing limited sanctions available in electronic communities).

The second criterion is also met when nobody in the traditional community really cares what the internal community does. For instance, while no one in the larger society or political system really cares about the rules for earning merit badges in the Boy Scouts, or the seniority rules in a collective bargaining agreement, members of the internal communities do. When no one cares, it is easier to defer to self-governance.

1. RULES:

Both the need for, and the indifference to, specialized rules exist with respect to cyberspace. The most obvious example relates to purely technical issues, such as enhancements to basic e-mail, Internet routing, Web protocols, and to netiquette rules of subject matter for newsgroups.

The case is hard to make, however, that members of electronic communities should be subject to different rules with respect to conduct that causes harm outside their own communities. It is implausible to assume that no one in the surrounding community will care when members of the electronic community cause harm beyond the electronic community boundaries. The larger community will certainly insist that its rules, intended to address harm to its members, be enforced within electronic communities as well as elsewhere. Clear examples are copyright infringement and use of domain names that conflict with trademarks.

A second possibility for independent rules involves contract formation. The members of an electronic community could agree that contracts for the sale of goods or services could be formed in a particular way.[11] For example, members could agree that exchange of electronic data interchange (EDI) transaction sets, or of tokens satisfying a predefined standard (for authentication using public key encryption)[12] forms a contract.

---

11. *See* RESTATEMENT (SECOND) OF CONTRACTS § 30 (1979) (permitting the offeror to specify how the offer may be accepted). Under this rule, offerors in an electronic network community could all specify the same manner of acceptance. The result would be the same as a contract formation rule for the community, such as discussed in the text.

12. "Public key encryption involves mathematical algorithms that factor large numbers. Through the use of appropriate algorithms, it is possible to obtain two numbers, called *keys*, one of which creates an encrypted message from plain text, and the other of which recovers the plain text from the encrypted version. One of these keys is held by a user of the technique and not disclosed to anyone else. This is called that user's *private key*. The other number, a key associated with the private key, is disclosed publicly. This is that user's *public key*. The public and private keys can be used together either to protect privacy in the content of a message, or to construct digital signatures ... or both."

A third possibility would be to have specialized rules for potentially offensive communications including obscene and pornographic communications. The rules could require that such communications be directed to particular parts of the electronic community, access to which is limited so as to admit only those over a certain age.[13]

Fourth, rules for payments could prescribe how offers, acceptances, and payment orders are to be authenticated, and how the risk of forgery and insolvency are to be borne. The result would be like bank clearinghouse rules.

2. PROCEDURES:

Electronic communities need specialized adjudicators to produce better results at a lower cost. Different adjudicatory results could arise from the use of specialized decision-makers in electronic communities. Specialized adjudicators could understand specialized rules for electronic communities better than adjudicators in larger communities who have less contact with the specialized rules. Specialized adjudicators could also understand particular factual contexts within which disputes arise over rule application. For example, a dispute might arise over loss-allocation under an electronic community payments rule. In such a case, an adjudicator who understands public key encryption would be in a better position to appreciate fault in the handling of public and private keys resulting in a forgery. Or, a specialized adjudicator could appreciate the failure of the manager of a reserved area to give notice of potentially offensive contents in the manner prescribed by the community rule. In such a specialized "zoning" case, knowledge of the workings of the boundaries of newsgroups and Web spaces would improve decision-making.

C. Open networks escape enforcement of conventional rules

Self-governance may be desirable because it is impractical to apply rules of larger communities.[14] One situation in which the impracticability

---

HENRY H. PERRITT, JR., LAW AND THE INFORMATION SUPERHIGHWAY 394 (1996) (emphasis in original) [hereinafter PERRITT, INFORMATION SUPERHIGHWAY].

The public and private keys can be used together either to protect privacy in the content of a message, or to construct digital signatures ... or both." *Id.* at 394.

13. *But see* Reno v. American Civil Liberties Union, 117 S.Ct. 2329, 2336-38 (1997) (stating that such verification mechanisms were "effectively unavailable to a substantial number of Internet content providers." (citations omitted)).

14. A similar situation led to the development of certain rules in admiralty. *See* Gordon W. Paulsen, *An Historical Overview Of The Development Of Uniformity In International Maritime Law*, 57 TUL. L. REV. 1065, 1066-67 (1983) (history of admiralty shows

criterion is satisfied is when the boundaries of electronic communities cross the geographic boundaries of traditional sovereigns. This occurs with rapidly increasing frequency as the Internet becomes the model for computer networks, handling a wide variety of commercial and personal communications and delivering commercially valuable information and services. In such network communities, harm occurring in one geographically defined jurisdiction frequently results from conduct occurring in a different geographically defined jurisdiction.

Internet transactions regularly cross national boundaries. [15] Such cross-border communications raise questions of the enforceability of export restrictions, the limitations on public access to public information, intellectual property protection, and the liability for injurious content.

The international nature of these transactions create problems that cannot be dealt with by traditional legal systems. Even if a jurisdiction in which the injury occurs asserts jurisdiction and chooses a plausible body of substantive law, it may lack the means of enforcing its decision, because the actor is somewhere beyond its reach. When conduct traditionally considered criminal is involved, the problem is more acute because of the absence of transitory crimes in traditional jurisprudence.[16] It is unusual for geographically defined legal systems to prosecute for crimes committed in other places, except by artificially redefining the place of commission to be the place of injury.

---

that the motivation for a separate legal system was the need of commerce for international uniformity).

15. This international characteristic is true not only of the Internet; it is also true of multinational businesses. However, the Internet poses greater problems for traditional law enforcement because it permits the effects of conduct occurring elsewhere to be felt within a traditional state without any conduct occurring in that state. Usually a multinational business has some physical presence in the state where its effects are felt.

16. *See* State v. Jones, 443 A.2d 967, 970 (Md. Ct. Spec. App. 1982) (courts of one state may not hear prosecution for crime committed against laws of another state); Bruce Church, Inc. v. United Farm Workers, 816 P.2d 919, 926 (Ariz. 1991) (distinguishing civil and criminal practices); State v. Miller, 755 P.2d 434, 436 (Ariz. 1988) (international law determines whether state may impose criminal penalties for conduct occurring elsewhere). *But see* Lauritzen v. Larsen, 345 U.S. 571, 585 (1953) (law of flag covers even criminal conduct under maritime law); United States v. Noriega, 746 F. Supp. 1506, 1512 (S.D. Fla. 1990) (state may criminalize conduct occurring elsewhere but having effects in prosecuting jurisdiction); Rios v. State, 733 P.2d 242, 244 (Wyo. 1987) (state may prosecute for child custody offense committed elsewhere by actors never within state when effects are felt on custodial parent in state); State v. Mazzadra, 258 A.2d 310, 314 (Conn. 1969) (holding that theft of automobile was a transitory crime for which defendants could be prosecuted in Connecticut although the theft occurred in New York).

Electronic network communities, on the other hand, may find it much easier to enforce rules. For electronic networks in which the attachment is primarily social, threat of exclusion from the network may be a powerful enough incentive to induce compliance with the rules. For electronic networks in which the attachment is primarily economic, the growing availability of low transaction cost methods of making payment potentially facilitate enforcement. A large producer may be required to post a bond, as for certification authorities used in digital authentication systems. Smaller participants, like consumers, are likely to have credit on the network, either through having paid for cybermoney or having arranged for secured electronic credit card transactions. A condition of network participation could be that the consumer must place some of this credit at risk in order to enable fines or civil penalties to be imposed through appropriate adjudicatory procedures.

Self-governing electronic communities can use these methods to deal with conduct occurring in their communities regardless of the place at which it occurs. Also, electronic communities can impose punishments and effectuate compensatory remedies regardless of the geographic place where the community member engaging in the conduct violating the rule is found.

D. Self-governance promotes voluntary compliance

An important advantage of democratic or other representative political systems from a utilitarian perspective, is that they are more likely than authoritarian systems to induce voluntary rule-compliance by citizens. This is so not only because of greater participation by those bound by the rules, but also because specialized rules are less likely to produce bizarre results than general rules drawn from traditional communities. Compliance with the rules imposed by surrounding legal systems may be low in certain electronic communities because the rules are not perceived as fitting the realities of the communities, or because enforcement of the rules by the regular legal institutions is impractical. In either or both of these situations, compliance may improve with standards of behavior that are acceptable to (while not identical to the rules of) the surrounding community, if a measure of self-governance is allowed to participants in the electronic communities. For instance, electronic community participants who wish to exchange messages containing potentially offensive content, might be willing to comply with rules requiring clear notice, the exclusion of minors, and other restrictions on access, while they would be unwilling to comply with prohibitions on exchanging such messages.

E. Conclusion

The likelihood of autonomy for electronic communities is greatest when specialized rules and adjudicators are needed, and traditional communities are indifferent to their content. In such situations, the inherent likelihood that a specialized legal system will be more efficient, that it will induce greater voluntary compliance, and that it will regulate behavior that otherwise would escape regulation, tilt the political balance in favor of autonomy.

IV. IS SELF-GOVERNMENT LEGALLY FEASIBLE?

All modern legal systems proceed from the foundational premise that only entities possessing sovereignty can make, apply, and enforce law. Despite the association of sovereignty with national governments, the reality is that governance is dispersed among a rich variety of public and private institutions. Most people in industrialized society work for employers who administer private systems of workplace governance. Most money moves in complex clearinghouse systems set up and administered by private banks. Most industrial production and commerce takes place in private contractual webs. Much social and religious life transpires in private associations. The increased importance of international human rights, trade, and environmental law has drawn upon the energy and expertise of thousands of non-governmental organizations (NGOs), such as Amnesty International and Greenpeace, to provide information and analysis to treaty based institutions.

In theory, however, these private governments derive their power from the traditional sovereigns and are always subject to the sovereign imposing new regulations and enforcing them. The relationship between private governments and traditional sovereigns is determined by traditional laws or regulations enacted by traditional sovereigns, by constitutions defining the power of traditional sovereigns, or by international treaty.

Self-governance can be realized in at least three forms: (1) immunity from the application of surrounding legal standards, (2) immunity from the enforcement power of traditional legal institutions, and (3) recognition of the prescriptive and adjudicatory acts of the autonomous community.

The feasibility of self-government depends on the traditional community's respect for, and deference to, community law. Traditional communities generally respect party autonomy exercised through contractual agreements. Thus, respect for community law can be earned by having a contractual framework for electronic communities. Although the enforcement of contractual autonomy may depend on traditional institutions, such dependence can be mitigated by internalizing

enforcement. The crucial elements of a self-governing community are completeness, the availability of coercive power to enforce community decisions, and a contractual framework expressing the norms, procedures, and institutional competencies.

A. Basic legal frameworks

Assessing the feasibility of autonomy for private electronic communities requires an understanding of the points of tangency between these communities and traditional sovereigns—the scenarios in which someone challenges the autonomy of the private community in the courts of traditional sovereigns. Ultimately, autonomy for private communities depends on comity being afforded them by traditional sovereigns,[17] which in turn is more likely if the private communities are "complete," in the sense that they offer the entire spectrum of rulemaking, adjudication, and enforcement.

Political autonomy originates in physical power. Nation-states are politically autonomous because they have the military power to keep themselves that way. The geographic scope of political units has historically depended on the reach of military technology, and the social cohesion necessary to use it. Sovereignty is formally associated with nation-states that have the practical ability to assert physical power to coerce compliance with their law within defined borders and with respect to a defined class of persons.[18] New nations, such as Bosnia-Herzegovina,

---

17. "Comity ... is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws." Joel R. Paul, *Comity in International Law*, 32 HARV. INT'L L.J. 1, 8 (1991). Mr. Paul criticizes comity as an imprecise concept, meaning little more than choice of law to some analysts, a discretionary doctrine of public international law to others, and a basis for insisting on reciprocity for still others.

18. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 201 (1987) ("Under international law, a state is an entity that has a defined territory and a permanent population, under the control of its own government, and that engages in, or has the capacity to engage in, formal relations with other such entities.").

Under international law, a state has:

(a) sovereignty over its territory and general authority over its nationals;

(b) status as a legal person, with capacity to own, acquire, and transfer property, to make contracts and enter into international agreements, to become a member of international organizations, and to pursue, and be subject to, legal remedies;

(c) capacity to join with other states to make international law, as customary law or by international agreement.

are created, and old nations such as the Soviet Union, disappear, but the birth of a sovereign state is a momentous occasion in diplomacy and international law.

Network communities quite clearly are not entitled to status as traditional sovereigns because they lack a defined territory, a permanent population, and mechanisms for exerting physical coercive power.[19] But new sovereigns can be created by delegation of power from traditional sovereigns. The European Union and the United States came into existence as sovereign entities through delegation of powers from nation-states through treaties and constitutions. Such delegation for network communities is, however, unlikely to occur within the foreseeable future.

Smaller, more or less autonomous communities, have long existed within power-maintained sovereign political units. Their establishment and continued existence has always depended on the sufferance of the sovereign. For example, fairs, cities, universities, and guilds existed under English law because of the grant of patents from the King. The patent defined the powers of the community it authorized.[20] This type of

---

Id. at § 206. "Sovereignty" is a term used in many senses and is much abused. As used here, it implies a state's lawful control over its territory generally to the exclusion of other states, authority to govern in that territory, and authority to apply law there. "The sovereignty of a state is reflected also in immunity for the state and its public property from certain exercises of authority by other states." *Id.* at § 206, cmt b.

19. "The Second Circuit has limited the definition of 'state' to entities that have a defined territory and a permanent population, that are under the control of their own government, and that engage in, or have the capacity to engage in, formal relations with other entities." Kadic v. Karadzic, 70 F.3d 232, 239 n.2 (2d Cir. 1995) (quoting Klinghoffer v. S.N.C. Achille Lauro, 937 F.2d 44, 47 (2d Cir.1991)).

20. "[T]he settlers had emigrated from an England that was localist in political organization: early seventeenth-century English towns, boroughs, counties and guilds still operated to a great extent as self-governing (although partially overlapping) entities." Jeremy Elkins, *University of Chicago Law School Roundtable Conference: Constitutions and "Survivor Stories" Declarations Of Rights*, 3 U. CHI. L. SCH. ROUNDTABLE 243, 255 (1996); *see also* Joan C. Williams, *The Invention Of The Municipal Corporation: A Case Study In Legal Change*, 34 AM. U. L. REV. 369, 374 (1985):

> Groups that the law identified as aggregate corporations seem unrelated to the modern eye: chartered boroughs, companies of merchants, including guilds, and universities. What did these groups share that caused them to be identified as corporations, while other groups, such as villages and towns, were not? The answer is that 'incorporated' entities were corporations because they shared a special relationship to feudal society: each of the major English 'corporations' developed from the late feudal practice of granting charters to groups that wanted to 'opt out' of feudal obligations. This division between groups that were corporations and

delegation exists in modern legal systems in the form of corporate and municipal charters. More generally, other types of private communities exercise a form of sovereignty under contracts mutually delegating attributes of sovereignty retained by the community members. The traditional sovereign allows this kind of private sovereignty by allowing freedom of contract. However, such community autonomy is dependent on the traditional sovereign for its very existence. It exists only if traditional sovereign institutions recognize the community's autonomy.

Let us examine what would happen if there were to be a clash between an autonomous electronic community and the traditional community in which it sits. Assume a deputy sheriff shows up at the door to seize a computer, to demand copies of certain files, or to arrest a natural person for certain conduct. Members of a network community are unlikely to prevail in physical resistance to the deputy sheriff. The law enforcement agent almost always can call upon superior force. The community enjoys autonomy only because it can claim privileges or immunities recognized by the traditional sovereign. For instance, if the deputy sheriff intrudes, the autonomous community prevails in a subsequent legal proceeding for trespass, conversion, or violation of civil rights.

But community autonomy is rarely a bilateral test between the traditional sovereign and the private community. It usually involves a three-way contest between private interests in which the traditional sovereign is the arbiter. The deputy sheriff in the hypothetical was sent by a court and acted pursuant to a writ or warrant. The warrant or writ was issued by a traditional sovereign's court on the request of a private plaintiff or public prosecutor acting on a private complaint. The prosecutor acted pursuant to authority granted by the traditional sovereign. The private plaintiff may be from within the community or from outside it. The community-autonomy question may have been tested long before the sheriff showed up at the door of the electronic community. In such cases, one party seeks to deny community autonomy. For example, an electronic association sued by a present member asserting a violation of its constitution, would defend on the grounds that the court in which the suit is filed must defer to internal

---

groups that were not was the second anachronistic aspect of English corporation law.

See also Joel Edan Friedlander, *Corporation And Kulturkampf: Time Culture As Illegal Fiction*, 29 CONN. L. REV. 31, 76 (1996) (explaining the conflict between the view that groups such as corporations enjoy status as actual person and the orthodox view that they are artificial persons with only such existence as is recognized by the traditional states).

tribunals on constitutional issues.[21] In other words, it asserts adjudicatory autonomy, while the private plaintiff asks the traditional court to deny autonomy of the private tribunals by deciding the case on the merits. A member of the electronic community accused of intellectual property infringement would defend on the grounds that the court in which the lawsuit is brought must defer to community rules which grant her a privilege with respect to the intellectual property, while the plaintiff claims that any contractual privilege is voided by traditional sovereign law on intellectual property. A criminal defendant would defend on the grounds that the traditional criminal statute should be interpreted with deference to electronic community rules, while the prosecutor on behalf of the victim would argue that no such deference is appropriate.[22] Less conventionally, the defendants may assert that they are immune from suit or from prosecution because of their community membership and the nature of the claim, while the plaintiffs appeal to traditional sovereign authority and deny the existence of immunity.[23]

---

21. *See, e.g.*, Blackshire v. NAACP, 673 N.E.2d 1059, 1061 (Ill. App. 1996) (reversing trial court for inappropriately interfering in internal affairs of private association; law of private associations requires judicial deference to authorized decisions of internal bodies); Georgopoulos v. Teamsters, 942 F. Supp. 883, 895 (S.D.N.Y. 1996) (holding that federal statute does not authorize judicial intervention into internal union affairs except when necessary to enforce minimum statutory standards).

22. *See, e.g.*, United States v. Morris, 928 F.2d 504, 509 (2d Cir. 1991) (defining criminal conduct in terms of what is authorized by private computer system). The suggested defense also might arise if a pornography prosecution were defended on the grounds that the electronic community defines the standards and that the material was not pornographic under those standards.

23. There are several types of immunity. The most basic type is sovereign immunity. Such immunity was rooted in the "perfect equality and absolute independence of sovereigns." Schooner Exchange v. McFaddon, 11 U.S. (7 Cranch) 116, 137, (1812). In recent decades, the former absolute view of sovereign immunity has evolved into a restricted view, which accommodates the reality that many sovereigns engage in commercial activities, as to which they should not necessarily be treated as states. *See generally* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 451 intro. note (1986) (providing immunity to states from the jurisdiction of the courts of other states, except for "claim arising out of activities of the kind that may be carried on by private persons"). Considerations of judicial administration supplement international law in immunizing certain witnesses and chattels from service of process or execution. *See* RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 83 (1969). Charities historically were immune from tort liability based on the rationales that their resources should not be diverted from charitable purposes, that the doctrine of respondeat superior was inapplicable, or that persons accepting benefits from charities waived tort claims. *See* RESTATEMENT (SECOND) OF TORTS

Such trilateral contests arise in several relevant contexts:

- conduct by community members that harm the legally recognized interests of nonmembers (e.g. defamation or intellectual property infringement);[24]
- intra-community conduct that offends non-waivable traditional community standards (e.g. racial, gender, or disability-motivated adverse decisions, or life- or personal-injury-threatening conduct within the community);[25]
- denials of membership under circumstances that would constitute a legal wrong under traditional law,
- expulsions from membership and post-expulsion efforts to collect fines or penalties from past members that would either offend traditional legal standards or would necessitate resort to traditional legal institutions for enforcement.[26]

In several of these examples, it is a member of the autonomous community who seeks to avoid self-governance. A community member may go "outside" because she thinks that traditional institutions, procedures, or substantive law will give her a better result on an access, authorship, or authentication issue.[27] For example:

- a present member of the association files a lawsuit in a traditional court asserting breach of contract based on an alleged violation of the association's constitution;

---

§ 895(e) & cmts. (1979) (reviewing history and justifications for immunity and repudiating it as a general rule).

24. *See, e.g.*, United States v. LaMacchia, 871 F. Supp. 535, 536-37 (D. Mass. 1994) (example of the use of anonymous file transfer protocol area to exchange software violating copyrights of non-participants); Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 139-42 (S.D.N.Y. 1991) (use of computer service to defame non-participant).

25. *See, e.g.*, United States v. Alkhabaz, 104 F.3d 1492, 1493 (6th Cir. 1997) (use of electronic mail system to discuss abduction of classmate).

26. *See, e.g.*, Cyber Promotions, Inc. v. Apex Global Info. Serv., Inc., No. Civ.A 97-5931, 1997 WL 634384 (E.D. Pa. Sept. 30, 1997) (granting preliminary injunction against termination of service to mass mailer in violation of Internet access service contract); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1028 (S.D. Ohio 1997) (granting preliminary injunction enjoining mass mailer from sending unsolicited advertisements to subscribers); Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 456, 459-60, 464-65 (E.D. Pa. 1996) (denying preliminary injunction against use of tool allowing subscribers to block junk e-mail).

27. *See* Perritt, *Community Regained*, *supra* note 7, at 991 (explaining that controversies over access, authorship, and authentication are the major ones requiring legal attention as the national information infrastructure develops). Authentication includes electronic signatures and other protections against forgery and repudiation of legally significant messages.

- a member of the association files a lawsuit in a traditional court alleging that the association's conduct violates a statute newly-enacted by a traditional legislature which explicitly applies to association conduct.

Outsiders also have grievances against communities and their members. What happens when an outsider wants access but is denied? What happens when an outsider infringes intellectual property generated within the electronic community? What happens when an outsider masquerades as a member and gets involved in an authentication controversy? Some examples of this are:

- a nonmember brings a lawsuit against a member of the association for intellectual property infringement;
- a prosecutor from a traditional jurisdiction commences a criminal prosecution against an association member for intra-association conduct that prima facie violates a traditional criminal statute.

The need to define boundaries between traditional sovereigns and autonomous private communities is analogous to the need to resolve inter-sovereign conflicts in international law.[28] The question of community autonomy in cyberspace depends upon whether the court to which the claim is presented defers to community law, either by recognizing an immunity for a particular defendant (unlikely) or by recognizing community substantive or procedural law. Often the question of autonomy is a choice of law question. Should the non-community court apply its own law (or the law of another conventional sovereign), or should it apply community law?

It is useful to consider how such situations are dealt with in the international realm. Boundaries of autonomy in international law are defined by the jurisdiction to prescribe,[29] the jurisdiction to adjudicate,[30] and the jurisdiction to enforce.[31] These three types of jurisdiction are useful benchmarks for private communities as well.

---

28. *See id.* at 1009.

29. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 401(a) (1987) (listing categories of jurisdiction); *id.* at §§ 402-03 (listing bases of and limitations on jurisdiction to prescribe); *id.* at § 461 (immunity of foreign state from jurisdiction to prescribe).

30. *See id.* at § 401(b) (1987) (describing jurisdiction to prescribe); *id.* at § 421 (describing jurisdiction to adjudicate); *id.* at § 451 (describing the immunity of a foreign state from jurisdiction to adjudicate).

31. This tripartite classification of types of jurisdiction is an innovation of the third Restatement of Foreign Relations. *See id.* at § 401 rptr. nt. 2 (1987). The second Restatement subdivided jurisdiction into the jurisdiction to prescribe and the jurisdiction to enforce. *See* RESTATEMENT (SECOND) OF FOREIGN RELATIONS § 6 (1965); *see also* Laker

Respect for electronic community law depends upon the electronic community having a contractual framework sufficient in scope to bind those wishing to avoid the effect of community decisions. Communities stand a better chance of being recognized either as sovereigns or as contractual communities if they offer relatively complete legal systems of their own. Incomplete systems must rely on traditional legal systems to perform the missing functions. To the extent that such external dependence exists, the community is less autonomous. Completeness, and thus autonomy, depends upon the capacity to perform functions essential to any legal system. As Joseph Raz has observed, "[t]he three most general and important features of the law are that it is normative, institutionalized, and coercive."[32] Cyberlaw—the legal system of electronic communities—is eligible for recognition as a separate legal system to the extent that it contains these three features. Electronic communities must offer normative rules for conduct; they must institutionalize rulemaking and rule application; they must sanction rule violators.[33]

Professor Hart observed that legal rules fall into one of two classes: primary rules, which impose duties; and secondary rules, which define powers to make and apply primary rules.[34] Primary rules pertain to the normative dimension. Secondary rules institutionalize and channel coercive forces. Cyberlaw is a complete legal system to the extent that it has both types of rules. Any claim for self-regulation in cyberspace must be tested according to these criteria—the existence of rulemaking, adjudication, and coercive enforcement means.

Airways, Ltd. v. Pan American World Airways, Inc., 604 F. Supp. 280, 292 (D.D.C.), *aff'd*, 731 F.2d 909 (D.C. Cir. 1984) (relating comity to extent of jurisdiction to prescribe, adjudicate, and enforce); Joel P. Trachtman, *Conflict of Laws and Accuracy in the Allocation of Government Responsibility*, 26 VAND. J. TRANSNAT'L. L. 975, 1046 n.288 (1994) (describing the three components of jurisdiction recognized by the Restatement); Christopher C. Joyner & Wayne P. Rothbaum, *Libya and the Aerial Incident at Lockerbie: What Lessons for International Extradition Law?*, 14 MICH. J. INT'L L. 222, 234-38 (1993) (using three bases of jurisdiction to explore extraterritorial application of United States law); Bruce Zagaris & David R. Stepp, *Criminal and Quasi-Criminal Customs Enforcement Among the U.S., Canada and Mexico*, 2 IND. INT'L & COMP. L. REV. 337, 338-42 (1992) (discussing bases of jurisdiction in U.S. and Mexican Law).

32. Joseph Raz, The Concept of a Legal System 3 (2d ed. 1980).

33. Offering normative rules is an assertion of jurisdiction to prescribe. Formalizing mechanisms for rulemaking and rule application involve assertion of jurisdiction to prescribe and to adjudicate, respectively. Sanctioning rule violators asserts jurisdiction to enforce.

34. *See* H.L.A. HART, THE CONCEPT OF LAW 78-79 (1961). Hart's secondary rules define legislative (rulemaking) and adjudicatory institutions and powers.

B. Contract: the framework for autonomy

Private contract is the most appropriate source of autonomy for electronic communities. Indeed, treaties and constitutions, the traditional sources of sovereignty, can be understood as contracts among sovereign states and sovereign people respectively. Most of the examples of private legal communities reviewed in Part IV involve private contractual webs to define the community and to allocate legal power within it.

Much can be done through conventional contracts to set up communities to which sovereigns will defer. Bank clearing house systems, WESTLAW licensing agreements, and collective bargaining agreements are good examples of contractual arrangements that establish internal governance mechanisms for the parties to the contract. Assuming a valid contract can be formed among the members of an electronic community, as discussed in this section, such a contract can achieve the criteria identified by Raz: norms, institutionalization, and coercion. A community contract can set specialized standards for conduct within the community. By providing for arbitration, such a contract can arrange for application of these rules through specialized community institutions. Indeed, it can arrange for on-line, cyberspace-based common law courts through appropriate arbitration clauses. Such a contract can also provide directly for coercive enforcement, by specifying liquidated damages, by requiring posting of a bond against which penalties may be imposed, or by providing for expulsion from the community (with or without forfeiture of property left within the community, e.g., intellectual property). In other words, contracts can provide the framework for a complete legal system.

Most of the models of self-governance[35] (all except the military one) depend upon private contracts as the normative, institutionalizing, and (to a lesser extent) coercive source of law. Even constitutional and international arrangements use documents similar to contracts in some ways to express the delegated powers. Parties to purely private contracts can achieve some immunity from outside legal institutions by waiving application of traditional law and recourse to traditional legal institutions. Thus, contract principles are a natural starting point for the establishment of an independent electronic community.

But the contractual nature of some electronic communities may be problematic.[36] Some electronic communities are anonymous, have

---

35. *See infra* Part VI.

36. Autonomy based on contract requires the presence of the elements of an enforceable contract: capacity to contract, offer, acceptance, and consideration. *See* PERRITT, INFORMATION SUPERHIGHWAY, *supra* note 12, at 379 (explaining the formal prerequisites of contractual obligation).

rapidly shifting membership, and may exist for any particular member only for as long as it takes her to send a request to a World Wide Web or news server and receive an item of information as a response. In these communities, there is no negotiation and no ongoing social relationship. There may be a contract, but it may be so brief in duration that it may be an intellectual stretch to say that the consumer of these services joins a community and agrees to participate in self-government. In this type of electronic community, contractual models associated with standard form contracts unilaterally issued by one party are most relevant.[37] This is because one party in these anonymous electronic communities will almost certainly publish the electronic equivalent of a standard form contract to which the participants will become parties to some extent. Standard form contracts have become inevitable as managerial direction has replaced market forces for a vast range of commercial transactions.[38] Professor Rakoff describes the reality that consumers almost never read the terms of standard form contracts, and that it would be eccentric to insist on changes. The drafting organizations would almost certainly not agree to changes,[39] and neither the drafting organization nor the consumer really expects the lawyer-crafted terms of the standard form to be followed.[40] In these settings, it may be unclear whether someone involved with community resources really is a "member" of the community, subject to its normative rules, institutions, and enforcement mechanisms, and within any shield of immunity and deference.[41]

In these circumstances, Professor Rakoff and others have suggested new rules of contract enforcement. Professor Slawson suggested that the standard terms in a form contract be enforced only when they are consistent with the reasonable expectations of the parties.[42] Slawson would determine the reasonable expectations according to the nature of the transaction. Both Slawson and Rakoff reviewed leading cases

---

37. *See* W. David Slawson, *Standard Form Contracts and Democratic Control of Lawmaking Power*, 84 HARV. L. REV. 529, 530, 532 (1971) (estimating that standard form contracts account for 99 percent of all contracts made).

38. *See* Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1173, 1223 (1983).

39. *See id.* at 1225.

40. *But see* ProCD v. Zeidenberg, 86 F.3d 1447, 1455 (7th Cir. 1996) (enforcing the terms of shrink-wrap license).

41. *See* Perritt, *Dispute Resolution*, *supra* note 7, at 352.

42. *See* Slawson, *supra* note 37.

explaining how their suggestions are not revolutionary departures from what courts actually do when confronted with standard form contracts.[43]

Making standard contracts unenforceable, however, engenders uncertainty. A better approach may be to construct a different contract regime, in which contract terms posted in some formal way and subject to review or challenge might be presumptively valid, but not otherwise. This approach borrows the concept from insurance regulation that the standard contract is generally subject to review by the insurance commissioner before it can be used with purchasers of insurance. It also borrows from ERISA,[44] which requires that employee benefits plans be published and filed with the Department of Labor. Whenever someone offers a contract defining a self-governing electronic community, that person can specify the way in which the offer is to be accepted and can also indicate what sort of an exchange is sought by the offeror (by the content of the offer and the circumstances under which it is made).[45] The offer can specify that it may be accepted by conduct (for example, hitting the enter key on one's computer), or by making a promise (such as giving a credit card number representing an implied promise to pay a stated subscription fee).

When the party to whom the offer is addressed (the offeree) engages in the specified conduct or makes the promise, she accepts the offer.[46] Typically, this conduct or promise also constitutes the offeree's half of the desired exchange, frequently called consideration.[47]

C. The limits of contract

Notwithstanding the power of contract, the contract theory has important limitations as a source of community autonomy. One limitation is political and another is legal. Politically, contractual communities are porous and may be impermanent, as compared to

---

43. *See* Rakoff, *supra* note 38.

44. *See* 29 U.S.C. §§ 1021-24 (1994) (requiring publication and filing of employee benefit plans).

45. *See* RESTATEMENT (SECOND) OF CONTRACTS § 30, cmt. a ("The offeror is the master of his offer .... The terms of the offer may limit acceptance to a particular mode."); *id.* at § 60 ("If an offer prescribes the place, time or manner of acceptance its terms in this respect must be complied with in order to create a contract.").

46. *See, e.g., id. at* § 32, cmt. a ("In case of doubt an offer is interpreted as inviting the offeree to accept either by promising to perform what the offer requests or by rendering performance, as the offeree chooses.").

47. *See* JOHN EDWARD MURRAY, JR., MURRAY ON CONTRACTS, 51 (1974) (consideration noted among six essential elements to formation of a contract).

sovereign communities. Private disputes tend to drift into public forums. For instance, the private character of collective bargaining has been significantly eroded by an expansion of legislatively defined individual employee rights, enforced by public institutions.[48] Injured persons seek relief in whatever forums seem most likely to produce the relief they desire. When an injured person is outside an electronic community, that person will probably press for relief from traditional institutions.

This limitation of contract can be mitigated to some extent by internalizing the enforcement function. Then enforcement of private community norms does not depend on the willingness of a traditional court to enforce a contract; the private community enforces it directly. Internalization of the enforcement function reduces the dependence of the self-governing community on traditional legal institutions to enforce its decisions, although it may increase the possibility of legal liability in traditional forums for the injury resulting from internalized enforcement.[49] The possibilities for internalized enforcement are greatly enlarged by the possibility of the privatization of Internet domain registration, under the International Ad Hoc Committee (IAHC) recommendations.[50] Someone who does not obey the rules or who flouts a decision can be denied an Internet domain name, effectively excluding him from the Internet (or at least from the part of the Internet within the scope of that domain registry).

The legal limitations on contracts concern the extent of comity; limits on the prescriptive jurisdiction of the private community. As Judge Posner once wrote, "If a consent decree provided that a violator could be punished by having his ears cut off, the judge could not sign it."[51] Despite the strong tendency for courts to enforce private arbitration agreements and arbitration awards, they are not enforceable when they contravene public policy.[52] Moreover, it is not clear that private arbitrators may be given authority to award punitive damages.[53] Further,

---

48. *See* Henry H. Perritt, Jr., Employee Dismissal Law and Practice 191-272 (3d ed. 1993).

49. Excluding someone from a subnetwork may constitute a breach of contract. Blocking someone's messages may be a tort. Collective enforcement may be a combination in restraint of trade in violation of the antitrust laws. *See infra* Part VII.B.1.

50. *See infra* Part V.C.

51. Donovan v. Robbins, 752 F.2d 1170, 1176 (7th Cir. 1985).

52. *See, e.g.*, United Paperworkers v. Misco, 484 U.S. 29, 43 (1987) (reversing refusal to enforce arbitration on public policy groups, but stating general principle).

53. See John Y. Gotanda, Awarding Punitive Damages in International Commercial Arbitrations in the Wake of Mastrobuono v. Shearson Lehman Hutton, Inc., 38 HARV.

contracts "in restraint of trade" are unenforceable,[54] and conduct undertaken pursuant to private contractual arrangements may produce tort liability.[55] The boundaries of self-government are determined by the scope of such liability, and by the limits of contract enforceability. Many of the limitations discussed above can be addressed by carefully designing a contractual system with all of the features necessary for a completely legal system, as per the Raz formulation. Hence, despite these limitations, contracting is the best way to achieve autonomy for electronic communities.

V. THREE EXAMPLES OF CYBERSPACE SELF-GOVERNMENT

Several forms of self-government already exist in cyberspace. Others have been proposed. The existing forms range from the (mostly) benevolent dictatorships exercised centrally by the proprietors of America Online (AOL) and Compuserve, to the much more loosely organized "netiquette" of Internet newsgroups. The newsgroup, alt.current-events.net-abuse (a.c.e.n.a.), is one of the most highly developed examples of the latter type of self-government. Proposals for a private, international mechanism for domain name registration by the International Ad Hoc Committee (IAHC) provide a comprehensive framework for self-government on a larger scope than has heretofore been experienced or proposed. Examination of both a.c.e.n.a. and IAHC's frameworks, and their comparison with the "royalist" frameworks operated by proprietary services, reveals some of the issues that must be confronted in any system of private self-government for cyberspace.

The legal frameworks for all three examples are contractual, explicitly in the case of America Online and the IAHC recommendations, and implicitly in the case of a.c.e.n.a. The contractual frameworks in all three cases are complete, in that they authorize rulemaking, adjudication, and enforcement. They contemplate coercive measures: termination of service by AOL, expulsion from the Internet by revoking domain names

---

INT'L L.J. 59, 61 (1997) (explaining that punitive damages in arbitration are allowed under United States law but not under many foreign sovereigns).

54. *See* 15 U.S.C. § 1 (1994).

55. *But see* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 141 (S.D.N.Y. 1991) (unsuccessful action against electronic information service for defamatory statements made under contractual arrangement); Zeran v. America Online, Inc., 958 F. Supp. 1124, 1128-35 (E.D. Va. 1997) (finding negligent defamation claim against information provider preempted; because statements made by party under contract with defendant); Religious Technology Center v. Netcom Online Communications Co., 907 F. Supp. 1361, 1383 (N.D. Cal. 1995) (denying summary judgment on contributory copyright infringement claim based on material posted under contract with defendant).

in the IAHC recommendations, and direct "killing" of messages in the case of a.c.e.n.a.

A. A.c.e.n.a.: an example of self-government[56]

A.c.e.n.a. is a democratic mechanism for enforcing certain netiquette rules against undesired postings popularly called "spam." The a.c.e.n.a newsgroup and several other conversation "forums" exist on a world wide conference and exchange system called USENET. Although often mentioned in conjunction with the Internet, USENET is a distinct system of cooperating Internet nodes; not all Internet nodes participate in USENET.[57] Each newsgroup addresses a particular subject. USENET developed a body of rules or conventions accepted by most traditional users, often referred to as "netiquette."[58] Commercial advertising violates netiquette, and frustrates the intent of USENET to channel communications into subject-specific groups.

Despite this netiquette convention, on April 12, 1994, the Phoenix-based law firm of Cantor & Seigel (C&S) sent a message (often called a "post") advertising its legal services to thousands of newsgroups. The response was virtually instantaneous, as thousands of users voiced their disgust in discussions on newsgroups such as news.admin.misc. and news.admin.policy. USENET subscribers were outraged by the

---

56. The research and initial drafting of this section was done by Sean P. Lugg, Villanova University School of Law, Class of 1996, December 19, 1997. Mr. Lugg is a law clerk to the author. For background information on a.c.e.n.a., see Scott Southwick, *The news.admin.net-abuse FAQ File* (visited Nov. 23, 1997) <http://www.bluemarble.net/~scotty/nana-history.html> and Scott Southwick & J.D. Falk, *The Net Abuse FAQ* (visited Nov. 23, 1997) <http://www.cybernothing.org/faqs/net-abuse-faq.html>.

57. USENET is a collection of several thousand discussion groups called "newsgroups." Participants in USENET feed newsgroup updates to each other, so that a human user can add a comment to a newsgroup by "posting it" on his own computer, and the USENET system then propagates that new posting and all others like it to other USENET computers so that within a day or so, the new postings are available on the newsgroup throughout the Internet. There is no entity that owns or controls USENET; it is a collection of cooperating computer administrators.

58. *See generally* Sally Hambridge, *Netiquette Guidelines* (visited Nov. 23, 1997) <http://www.cybernothing.org/cno/docs/rfc1855.html> (summarizing netiquette rules, including general rule against posting messages inconsistent with character of newsgroups or mailing lists).

commercialization of the system. C&S were "flamed"[59] by thousands who alleged, inter alia, violations of USENET conventions, and disregard for netiquette. Unaffected by these protests,[60] and realizing the vast, low cost advertising potential of the USENET,[61] C&S announced their intentions to form an advertising company, Cybersell.[62] Because flaming failed to end the practice, a search for other, more coercive, means was initiated.

A.c.e.n.a. was established on April 25, 1994 to channel concerns about such USENET abuses.[63] The most prominent assailant of identified "spam" is Cancelmoose(TM), an anonymous member of the newsgroup.[64] Operating from a European site, Cancelmoose effectively rids the network of bothersome postings by means of "cancelbots," [65] or cancel messages. A response is posted soon thereafter, notifying the newsgroup of the cancellation. Furthermore, a message is sent to the "spammer," the individual or group who posted the message, notifying him of the action,

---

59. "Flaming" is the practice of besieging an individual with electronic or paper mail to voice disagreement to a posted message.

60. Acting contrary to the beliefs expressed by a consensus of USENET users is a violation of USENET conventions. This proposition is inferable from the general rules of netiquette.

61. C&S were able to transmit their message to approximately 30 million users in less than 90 minutes, with modest cost to the firm.

62. C&S stated that their goal was to make commercial advertising pervasive on the Internet. To accomplish this goal, they planned to create the advertising company Cybersell. *See* Peter H. Lewis, *Arizona Lawyers Form Co. for Internet Advertising*, N.Y. TIMES, May 7, 1994 at A1.

63. The newsgroup alt.current-events.net-abuse was "chartered" on April 25, 1994, less than two weeks after the initial C&S post. A.c.e.n.a. was replaced in November 1996 by the news.admin.net-abuse.* groups. *See* Scott Southwick & J.D. Falk, *The Net Abuse FAQ* (visited Nov. 27, 1997) <http://www.cybernothing.org/faqs/net-abuse-faq.html>.

Although formed for discussion of net abuses generally, "spamming" is the only occurrence which has been deemed "net-abuse" by consensus. Although the definition of "spam" varies, the generally accepted description is "the same article, or essentially the same article, posted an unacceptably high number of times to one or more newsgroups." *Id.*

64. *See id.* Cancelmoose, who now has a home page on the Web—http://www.cm.org/—has left his original activities to others. *See* Scott Southwick & J.D. Falk, *The Net Abuse FAQ* (visited Nov. 27, 1997) <http://www.cybernothing.org/faqs/net-abuse-faq.html>.

65. *See id.*

the reasons for the action, and what steps to take in the future to avoid a similar occurrence.

The readership of a.c.e.n.a consists predominantly of news administrators who can set filters that control the flow of messages to and from the site. Cancelmoose's cancel messages contain a readily detectable signature which enables site administrators to screen the cancels if desired. There is widespread approval of the actions of Cancelmoose by those active in the newsgroup. Furthermore, those disapproving a particular cancel maintain the ability to disregard the cancel messages by reconfiguring the receiving site.[66]

B. Is A.c.e.n.a. fair?

A.c.e.n.a. is interesting because it exhibits attributes of rulemaking (deciding what the norms of acceptable use are), adjudication (deciding whether a particular message violates the norms), and enforcement (Cancelmoose's cancellation of messages determined to violate the norms).

The main questions with respect to rulemaking are not procedural; they concern representation. How does one know that an electronic group like a.c.e.n.a has legitimate rulemaking power? What is the likelihood that the views represented in that discussion group adequately reflect the views of those to be bound by the rules? One answer, of course, is that the a.c.e.n.a. newsgroup is accessible to anyone using the Internet, and only persons using the Internet will be bound by the rules. In other words, anyone who is bound had an opportunity to participate, and failure to participate is not a persuasive argument for not being bound.

The adjudicatory function is somewhat trickier. Needed flexibility could be lost if lawyers (and others) insist on imposing the details of a modern civil procedural system on the adjudicatory process in cyberspace. The usual question in evaluating adjudication is compliance with due process. To avoid the risk of violating due process, it is appropriate to consider the evolution of adjudication in the Anglo-American tradition. Such an evolutionary perspective reveals the flexibility of the due process concept. Initially, the adjudicatory decision-makers were persons with actual knowledge of the facts.[67] The earliest juries had virtually plenary power to decide the case, without the constraints of modern notions of the fact-law distinction, and they also

---

66. Cancelmoose's cancel messages contain identifiers that may be easily recognized and disregarded by proper configurations of the receiving computer system.

67. *See* F.W. Maitland, The Constitutional History of England 46 (1908).

were witnesses to the conduct giving rise to the dispute. So the basic idea was that the legal system gathered together a group of people from the community who had personal knowledge of what went on and then permitted them to decide whether the conduct should be punished. That is not too far removed from the situations in a.c.e.n.a when most of the participants of the discussion of a particular incident have seen the offending message for themselves.

It was not always feasible, however, to assemble a jury that already knew what went on. Thus, it was necessary to develop methods for the disputants to tell their stories to the adjudicatory decision-makers. There are, of course, a variety of ways of telling stories, some effective and some not, some faithful to the real facts and some not. The notion of story telling to the adjudicatory decision-makers gradually evolved into formal mechanisms for determining who is entitled to tell a story (usually a professional lawyer) and rules for deciding how the story could be told—rules of evidence. The core idea of the modern jury trial, however, is not to be found in the definitions of the legal profession or in the current versions of the rules of evidence or civil procedure. The core ideas are to be found in the concept of giving each side an opportunity to tell its story, so that the people with the greatest interest in developing the story fully from the two opposing perspectives can do so. With that as a guide, a.c.e.n.a can be evaluated more fully. Arguably, its openness permits both accusers and defenders of a message to tell their stories to the decision-makers—the net-administrator participants on a.c.e.n.a. Viewed thus, a.c.e.n.a. satisfies the test for fair adjudication.

The enforcement function is perhaps trickiest of all, because it is here that the risk of an unaccountable invasion of private rights is greatest. A private adjudicatory decision does little harm if there is no coercive enforcement. It is important that due process have occurred before the deprivation represented by enforcement. In this regard, it is useful to look to traditional approaches to private individuals' authority to arrest (seizure of the person) or to seize property pursuant to judicial decree. The Statutes of Winchester identified private individuals as significant actors in the criminal justice process.[68] The role of the private citizen extended beyond simply protection of his own possessions; individuals owed a duty to society to join in the attempts to apprehend

68. *See* M. CHERIF BASSIOUNI, CITIZENS ARREST: THE LAW OF ARREST, SEARCH, AND SEIZURE FOR PRIVATE CITIZENS AND PRIVATE POLICE 9 (1977). "The Statutes of Winchester, enacted in 1285, formalized much of England's practice in matters of criminal justice and rules of apprehension." Furthermore, "the role of private persons in criminal justice was significant." *Id.* at 9.

criminals.[69] Private citizen arrests, searches, and seizures have traditionally been upheld under statutory or common law principles of citizens' arrests.[70]

Cancelmoose acts pursuant to the consensus of the participants in a.c.e.n.a. The consensus formed in a.c.e.n.a. can be viewed as the equivalent of a combination of a jury verdict and a warrant or a judgment. Viewed thus, Cancelmoose is equivalent to a deputy sheriff executing an arrest warrant after a criminal conviction, or a private party actually under color of a judgment. Using such analogies, we can see that the enforcement mode of a.c.e.n.a. is legitimate and "fair."

The other side of the coin, however, is that Cancelmoose does not enjoy a status equivalent to that of a public officer such as a sheriff (a sheriff is not self-appointed). And the a.c.e.n.a. process "authorizing" Cancelmoose to act is much more fluid and informal than the highly formal process of receiving a jury verdict and entering judgment on it. These differences animate arguments that a.c.e.n.a. is not "fair."

C. Self-government institutions proposed by IAHC

In 1997, the International Ad Hoc Committee (IAHC) proposed a comprehensive plan for self-government in a limited subject-matter—Internet domain names. This plan, based on an international web of private contracts and backed up by arbitration, is the most comprehensive yet proposed for a private, international system of Internet governance.

The IAHC was formed at the initiative of the Internet Society (ISOC)[71] and at the request of the Internet Assigned Numbers Authority

---

69. *See id.* at 9 ("Not only was it the right of any person to apprehend offenders, there was also a positive duty to drop all work when the 'hue and cry' was raised, and to 'join immediately in the pursuit'; and a private person was required to take part in the community institution of the 'hue and cry.'" (quoting J. HALL, THEFT, LAW AND SOCIETY, 162 (2d ed. 1952)); *see also* John Simon, Note, Tennessee v. Garner: *The Fleeing Felon Rule*, 30 ST. LOUIS U. L.J. 1259, 1263 (1986) (describing historical practice of outlawry; once one was declared an outlaw, every citizen had a duty to apprehend, and if necessary, to kill the outlaw).

70. *See* BASSIOUNI, *supra* note 68, at 87-95 (providing an index of state citizen's arrest statutes).

71. See Donald M. Heath, *Written Testimony of Donald M. Heath to U.S. House of Representatives Committee on Science Subcommittee on Basic Research For: Hearing on Internet Domain Names* (visited Oct. 10, 1997) <http://www.house.gov/science/heath_9-30.html>; see generally Internet Society (last modified Oct. 8, 1997) <http://www.isoc.org/>.

(IANA).[72] In addition, the IAHC was supported by the Internet Architecture Board,[73] the International Telecommunications Union,[74] the International Trademark Association,[75] and the World Intellectual Property Organization (WIPO).[76] Beginning work in November 1996, the IAHC was to "define, investigate, and resolve issues resulting from international debate over a proposal to establish global registries and additional generic Top-Level Domains."[77] IAHC sought comments from a wide variety of people and organizations and issued a final report with associated draft legal documents in February 1997. This report recommended changes in top-level domains for the Internet and a complete reorganization of the mechanisms for administering Internet domain names. The constitutional document, the generic Top-Level Domain-Memorandum of Understanding (gTLD-MoU), was signed in Geneva on May 1, 1997 and deposited with the Secretary General of the International Telecommunications Union.[78] With the signing of the

---

72. *See generally Internet Assigned Numbers Authority* (visited Sept. 13, 1997) <http://www.isi.edu/iana/>.

73. "The [Internet Architecture Board (IAB)] is responsible for defining the overall architecture of the Internet ... . The IAB also serves as the technology advisory group to the Internet Society, and oversees a number of critical activities in support of the Internet." *The Internet Engineering Task Force: Glossary* (visited Oct. 11, 1997) <http://www.ietf.cnri.reston.va.us/glossary.html#IAB>.

74. *See generally International Telecommunication Union* (last modified Sept. 30, 1997) <http://www.itu.int>. The ITU is a treaty based upon inter-governmental organization, concerned with international telecommunications regulation. *See id.*

75. "[The International Trademark Association (INTA)] is an association of trademark owners and advisors worldwide. INTA is dedicated to the support and advancement of trademarks and related intellectual property concepts as essential elements of effective national and international commerce." *INTA Online* (visited Oct. 11, 1997) <http://www.inta.org>.

76. *See generally The World Intellectual Property Organization (WIPO)* (last modified Oct. 7, 1997) <http://www.wipo.org/eng/index.htm>. The World Intellectual Property Organization is a treaty-based intergovernmental organization providing a framework for multi-national negotiation of intellectual property treaties. *See id.*

77. Donald M. Heath, Written Testimony of Donald M. Heath to U.S. House of Representatives Committee on Science Subcommittee on Basic Research, For: Hearing on Internet Domain Names (visited Oct. 10, 1997) <http://www.house.gov/science/heath_9-30 html>.

78. The International Telecommunications Union is an entity with some advantages to nongovernmental participants because it permits full scale participation by such entities in its deliberations. This is not true of most international multilateral organizations.

gTLD-MoU, the IAHC was dissolved and replaced by the Interim Policy Oversight Committee (IPOC). As of May 15, 1997, 110 entities had signed or indicated their intent to sign the gTLD-MoU, although there is much controversy over the inclusion of some entities on that list.[79]

A Domain Name System (DNS) is an essential component in the Internet's operation. It permits use of human-friendly addresses for nodes connected to the Internet such as "kentlaw.edu," "law.vill.edu," "cilp.org," "fcc.gov," and "ibm.com."[80] The DNS functions through domain name servers that translate the human-friendly names into IP addresses (such as 153.104.15.250) through a series of interconnected domain name tables maintained on DNS servers. Tens of thousands of DNS servers are linked in a kind of hierarchical distributed look-up service.[81]

The IAHC was formed because of a growing set of controversies over the DNS as it now exists. The popularity and commercialization of the Internet has meant that multiple entities sometimes want to use the same domain name. Sometimes this occurs because the same few letters can signify more than one well known company, product, or service, or because some persons have registered domain names for the primary purpose of selling them to enterprises with which they appear to be associated. Many of the controversies relate to trademarks and service marks, as when enterprise A uses a domain name that is the same as a trademark registered to enterprise B. At the same time, Internet users outside the United States increasingly are restless with U.S. dominance of the DNS, a result of the Internet's origins in the U.S. Department of Defense.

The IAHC recommendations reflected the IAHC mandate to ameliorate conflicts over top level domains. They proposed a non-governmental solution to provide for competition among registries, and

---

79. See generally Donald M. Heath, *Written Testimony of Donald M. Heath to U.S. House of Representatives Committee on Science Subcommittee on Basic Research, For: Hearing on Internet Domain Names* (visited Oct. 10, 1997) <http://www.house.gov/science/heath_9-30 html>; The Generic Top Level Domain Memorandum of Understanding (visited Oct. 10, 1997) <http://www.gtld-mou.org/>. In private conversations with the author in the Summer of 1997, some entities shown as subscribed to the IAHC recommendations questioned whether they knowingly consented to be signatories.

80. The characters after the period in the examples given are Top Level Domains (TLD) signifying respectively two educational institutions, a non-profit organization, a United States governmental body, and a commercial enterprise.

81. If one DNS server does not know a domain name for which it is asked to supply the IP address, it refers the request to another DNS server with broader knowledge of that part of the Internet domain.

to develop an open process.[82] The recommendations addressed the administration of domain name assignments and the behavior of the distributed look-up service that maps human-friendly names into IP addresses. In addition to recommending the definition of seven new top-level domains, the IAHC report declared that "the Internet top-level domain space is a public resource." The administration of this public resource presents public policy issues, and should be carried out in an open and public manner "in the interest and service of the public."[83]

Of particular significance for this article, the IAHC recommended a new governance structure based on several memoranda of understanding, which both public and private sector entities were invited to sign. The gTLD-MoU—the constitutional document—became effective when it was signed by the IANA and ISOC. "Stewardship of the gTLD space was assigned to the gTLD DNS Policy Oversight Committee ("POC") comprising members named by the ISOC, IANA, [Internet Architecture Board], [International Telecommunications Union], International Trademark Association, WIPO and [the Council of Registrars]."[84]

Other memoranda created several regulatory bodies to carry out domain name policy. The Council of Registrars (CORE) was established by a Memorandum of Understanding (CORE-MoU), signed by multiple competing globally-dispersed registrars. CORE operates as a Swiss non-profit association. A gTLD DNS Policy Advisory Body (PAB) was formed from public and private sector consultation and oversees POC and CORE activities.[85] "Changes to policy can be initiated by POC and enabled upon the agreement of ISOC and IANA, with the review of PAB and CORE." One could regard the legislative initiative function as residing with POC, subject to revision and possible veto by PAB and CORE.

Two international treaty-based organizations also play a role in implementing the IAHC recommendations. The International

---

82. See generally Donald M. Heath, *Written Testimony of Donald M. Heath to U.S. House of Representatives Committee on Science Subcommittee on Basic Research, For: Hearing on Internet Domain Names* (visited Oct. 10, 1997) <http://www.house.gov/science/heath_9-30 html>.

83. *Final Report of the International Ad Hoc Committe: Recommendations for Administration and Management of gTLDs* (visited Sept. 13, 1997) <http://www.gtld-mou.org/draft-iahc-recommend-00.html>.

84. *See generally* Donald M. Heath, *Written Testimony of Donald M. Heath to U.S. House of Representatives Committee on Science Subcommittee on Basic Research, For: Hearing on Internet Domain Names* (visited Oct. 10, 1997) <http://www.house.gov/science/heath_9-30 html>.

85. *See Generic Top-Level Domain (gTLD-MoU) Technical Meeting* (visited Oct. 11, 1997) <http://www.gtld-mou.org/press/pab-2.html>.

Telecommunication Union agreed to act as the depository for the gTLD-MoU and to publish the list of signatories.[86] WIPO supports a dispute resolution mechanism for challenges of any domain name applicant's right to hold and use a second level domain name under the rules of the WIPO (Geneva) Arbitration and Mediation Center. WIPO would administer a new system of Administrative Domain Name Challenge Panels (ACPs). "These panels do not substitute for national or regional sovereign courts; they have authority over the domain names only, not the parties. Unlike courts, however, the challenge panels would have the ability to exclude certain names, such as world-wide famous trademarks, from all of the CORE gTLDs."[87]

Article 7 of the CORE-MoU reinforces WIPO's function. Registration agreements and application forms for assignment of secondary level domain names must include clauses that bind the registrars to follow ACP decisions and that bind applicants to submit to WIPO mediation, decision by an ACP and arbitration.[88] The WIPO Center must notify CORE of any results and decisions of ACP, mediation or arbitration proceedings that require action.[89]

Appendix D of the gTLD-MoU provides substantive guidelines for administrative domain name challenge panels. Under the gTLD-MoU, ACPs and the associated mediation and arbitration mechanism only have jurisdiction over claims regarding use of a second level domain name that is identical or closely similar to an alphanumeric string that is deemed to be internationally known and for which demonstrable intellectual property rights exist.[90]

---

86. *But see* Bruno Giussani, *Cybertimes: International Council to Take Up Issue of Domain Names*, N.Y. TIMES, June 18, 1997, at A1 (reporting on opposition to ITU role by Internet service providers).

87. *Final Report of the International Ad Hoc Committee: Recommendations for Administration and Management of gTLDs* (visited Oct. 11, 1997) <http://www.gtld-mou.org/draft-iahc-recommend-00.html>.

88. *See Memorandum of Understanding for the Internet Council of Registrars* ("Core-MoU") (visited Oct. 11, 1997) <http://www.gtld-mou.org/docs/cor-mou.htm>.

89. *See id.*

90. "Once an alpha numeric string has been deemed, for purposes of this policy, to be internationally known, and existing intellectual property rights have been demonstrated, an exclusion could be decided by an ACP, subject to consideration of rights held by others." *[Revised] Substantive Guidelines Concerning Administrative Domain Name Challenge Panels* (visited Nov. 7, 1997) <http://www.gtld-mou.org/docs/racps.htm>. These guidelines are reserved, pending further public discussion on the details of the Substantive Guidelines.

ACP procedures would allow for two types of exclusion. First, the second level domain name which was challenged could be excluded (that is, from the particular gTLD in which it was registered without the authorization of the owner of the intellectual property right). Second, a broader exclusion from some or all of the CORE gTLDs could be applied for, in 'exceptional cases.' Such cases would include at least trademarks which are globally known.[91]

Procedurally, any person can file a challenge requesting either exclusion or transfer of the requested second level domain name to the challenger.[92] Appendix D provides criteria for ACPs to determine if a challenge has been established successfully.[93] The ACP determinations, however, are of limited effect. "A determination of an ACP shall carry no precedential weight in any later national or regional court proceeding."[94] Appeals are permitted, although Appendix D is unclear as to what body has jurisdiction over the appeal. Presumably it is the same or another ACP.[95] Clearly, a de novo hearing by national or regional courts is contemplated.[96]

Unfortunately, the dispute resolution machinery proposed by the IAHC is limited to disputes over domain name assignment, especially those disputes that raise trademark or unfair competition issues. Moreover, it is an optional procedure, with a resort to national courts remaining available. As explained above, agreement on even this limited arrangement has been elusive. No doubt, agreement would be even harder to obtain with respect to a broader dispute resolution procedure and more ambitious use of domain names as leverage to enforce a broader set of international norms.

Notwithstanding these practical difficulties, it is useful to consider the possibility of using Internet domain names as a means of enforcing international norms in general. The growing importance of domain names in the Internet may provide the basis for a broader enforcement mechanism based on the IAHC recommendations, and may ultimately obviate the need for reliance on traditional legal institutions.

---

91. *Id.*

92. *See id.*

93. *See id.*

94. *Id.*

95. *See id.*

96. "Any dispute which has been submitted to an ACP may be brought, at any time before, during or after the administrative challenge procedure, to a national or regional court, which would hear the dispute under its normal jurisdictional and substantive rules." *Id.*

Would such a system work? Domain names as the centerpiece of a new private governance mechanism can serve some of the traditional purposes of legal remedies[97] reasonably well, but not others. On the one hand, revoking a domain name is a poor way of compensating a victim. Even if a domain name is awarded to a complaining party, that provides no compensation for past infringement of the trademark. There is nothing in the proposed IAHC machinery, no matter how far it is extended, that would serve the compensation purpose well. On the other hand, revocation will exclude the target from the Internet, and that possibility may have economic consequences serious enough to represent a major deterrent. If an entity believes it will be put out of business if it violates rules, it will avoid violating those rules. Finally, revocation of domain names is a very effective means of preventing further misconduct by the target; without a domain name, the target cannot repeat any further misconduct through the Internet.

A complete system for using domain name revocation as a remedy for enforcing international adjudicatory decisions requires at least three elements: rules for prescriptive jurisdiction, rules for adjudicatory jurisdiction, and rules for assuring compliance with the final order requiring that a domain name be revoked. The rules for prescriptive and adjudicatory jurisdiction have already been worked out.[98] Such rules are necessary to determine which substantive norms and which adjudicatory decisions would be entitled to enforcement through the domain name system. When the substantive norms and the adjudicatory decisions emanate from international institutions, their jurisdiction would be determined according to the documentary sources of their power. Currently, those sources are treaties.

That leaves the need to assure that the "sheriff" in this new legal domain obeys the "writ of execution." The obligation to obey the writ of execution would be expressed much as the obligation to obey decisions of ACPs and IAHC arbitration is expressed in the existing Memorandum of Understanding: once a decision to revoke a domain name is reached by the designated body, any registrar in the system must revoke the domain name. A registrar who declines to fulfill that obligation would lose its status as registrar. The integrity of this system depends upon the continued willingness of everyone within the hierarchical chain of

---

97. Remedies in law are intended to achieve at least three ends. First, damages compensate the victim. Second, remedies are intended to deter misconduct by punishing actors; knowledge of the possibility of such penalties deters misconduct. Third, remedies such as injunctions and incarceration are intended to block further misconduct by the actor.

98. *See supra* Part IV.A.

registrars to live up to their contractual commitments. As the scope of rules and decisions to be enforced by this means increases, however, the degree of compliance by registrars who intend to comply may diminish.

D. Economic royalism: proprietary power

Proprietary forms of private governance prevail in many parts of cyberspace. For example, a service provider such as America Online or CompuServe enforces unilaterally adopted rules by withdrawing the service of users who violate the rules. Most proprietary providers publish relatively complete sets of rules for use of the service.[99] Violation of the rules constitutes a trespass[100] and may justify termination of the service under contract.[101] Some proprietary providers use software tools that enforce the rules.[102] Use of a proprietary service over the objections of the proprietor is a trespass and is enjoinable.[103] Federal courts have deflected arguments that proprietary providers must provide access under the First Amendment of the United States Constitution or under the antitrust laws.[104] Thus, governmental authority in these situations is based on the power over private property.

Despite performance of these governance functions, proprietary services are not subject to constitutional constraints applicable to

---

99. *See* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1024 (S.D. Ohio 1997) (referring to policy statement limiting uses of service).

100. *See id.* at 1024 (granting preliminary injunction on trespass theory: connecting to Internet is no more a relinquishment of power over service provider's private property than any invitation to business customer is a relinquishment of power over inviter's premises).

101. *See* Cyber Promotions, Inc. v. Apex Global Info. Servs., Inc., No. Civ.A 97-5931, 1997 WL 634384, at *3 (E.D. Pa. Sept. 30, 1997) (recognizing general rule, but enjoining termination of service before expiration of 30-day contractual notice).

102. *See* Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 456, 459-60 (E.D. Pa. 1996) (describing software permitting users to block unsolicited e-mail); *CompuServe*, 962 F. Supp. at 1017 (describing orders to cease and desist, followed by use of software blocking devices).

103. *See* CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1017 (S.D. Ohio 1997) (granting injunction on trespass theory).

104. *See* Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 456, 457-58 (E.D. Pa. 1996) (reviewing result in earlier First Amendment ruling, and summarizing ineffectiveness of antitrust argument).

traditional governmental entities.[105] Nevertheless, to the extent it limits its power by contract, a proprietor must follow its own rules.[106]

If one has a purely contractual framework within which rules are made and enforced, as in the three cases cited in the notes to this section, the likelihood of state action is de minimis. The only remedy of someone disadvantaged by the private dispute resolver would be for breach of contract, as in *Apex*, or a related tort claim such as fraudulent misrepresentation or intentional interference with contractual relations. On the other hand, when the dispute resolution mechanism is sanctioned by statute, as in the Fair Credit Reporting Act, the situation looks more like *Flagg Brothers v. Brooks*,[107] where the self help repossession was sanctioned by Article 9 of the Uniform Commercial Code, as adopted by the New York legislature. But in *Flagg Brothers*, the Supreme Court held that private conduct within a framework established by statute insufficiently engages the power of the state to represent state action. State action occurs only when enforcement powers of the state are used by private entities. One of the strongest examples of private enforcement is the landlord's common law right of distress: the power and privilege of seizing personal property on leased premises as a remedy for tenant nonpayment of rent. Exercise of the distress remedy generally has not been viewed as constituting state action, unless officers of the state such as deputy sheriffs assist the landlord.[108] Thus, designers of private electronic governmental mechanisms have greater autonomy when their arrangements are purely contractual, and correspondingly less when the last step in the private process is resort to public judicial machinery.

E. Conclusion

Among the three patterns of Cyberspace self-governance that have begun to emerge, the a.c.e.n.a. approach is the most democratic, but tends toward anarchy because of low institutionalization and diffusion of coercive power. The proprietary approach avoids those vices but concentrates power in the hands of one party and provides few channels

---

105. *See id.* at 464.

106. *See Apex*, 1997 WL 634384, at *3 (granting injunction against termination of service, based on failure to observe contractual notice period).

107. 436 U.S. 149 (1978).

108. *See e.g.*, Smith v. Chipman, 348 P.2d 441, 442 (Or. 1960); *see also* Shane J. Osowski, *Alaska Distress Law in the Commercial Context: Ancient Relic or Functional Remedy?*, 10 ALASKA L. REV. 33, 45-48 (1993); Douglas Ivor Brandon et al., Special Project, *Self Help: Extra-Judicial Rights, Privileges and Remedies in Contemporary American Society*, 37 VAND. L. REV. 845, 937, 1040 (1984).

for involvement by service users. It represents a kind of economic royalism, that may invite resort to traditional institutions to limit the power of proprietors.[109] The best of the three is the contractual web proposed by the IAHC because it is complete, democratic, and provides an appropriate degree of institutionalization.

VI. COMPARISON WITH OTHER SELF-GOVERNING COMMUNITIES

A. Introduction

Many autonomous self-governing communities exist within or separate from national states. As noted above, most autonomous communities owe their existence to grants of power from the national sovereign. Sometimes the grant is explicit, as in royal patents for the City of London, the East India Company, or the American provinces of Pennsylvania and Maryland. Sometimes it is implicit, having evolved through the common law. For example, the common law has worked out a kind of prescriptive and adjudicatory autonomy[110] for religious orders and certain internal matters of corporate governance. The following sections examine several models of self-governing communities. Mechanisms of self-governance for the Internet are likely to draw on these models, including their mostly contractual frameworks and the bases for limiting their scope.

The interesting thing about the following models is that, unlike traditional sovereigns, their boundaries are rarely marked by geography. Rather, other techniques are used for defining community membership. Voluntary membership models rely on consent to represent acceptance of a contractual framework for self-governance. By contrast, involuntary membership models must rely on some other legal justification for binding members to community norms and decisions, even when the remainder of their structure is contractual.

In the following sections, each model is assessed against Raz's three criteria for legal systems: the existence of normative rules, the existence of institutions, and the existence of coercive mechanisms. These criteria map roughly into the prescriptive, adjudicatory, and enforcement modes

---

109. *See, e.g.*, Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 456 (E.D. Pa. 1996); Cyber Promotions, Inc. v. Apex Global Info. Servs., Inc., No. Civ.A. 97-5931, 1997 WL 634384 (E.D. Pa. Sept. 30, 1997).

110. Prescriptive authority is authority to make rules. Adjudicatory authority is authority to decide cases. *See supra* Part IV.A (considering prescriptive and adjudicative immunity in the international context).

of jurisdiction.[111] As the section on legal frameworks explained, complete legal systems—those possessing all there criteria—are more likely to achieve autonomy. In addition, the sections also illustrate the ways in which traditional sovereigns limit the boundaries of community power, while affording immunities to activities at the core of the communities.

B. Involuntary membership models

1. *COLLECTIVE BARGAINING MODEL*

Collective bargaining refers to the process of making and enforcing terms and conditions of employment and other workplace rules through institutions established by a contract (a collective bargaining agreement) negotiated between an employer or group of employers and one or more trade unions representing their employees. After a majority of the employees within a "bargaining unit" have selected a union representative, a collective bargaining agreement binds all the employees within the "bargaining unit" regardless of whether they would prefer to negotiate individual contracts of employment with different terms.[112] Thus, membership can be involuntary.

An employment relationship covered by collective bargaining is a strong example of a self-governing community under American law. Even though specialized agencies have been set up at the federal level to establish the boundaries of collective bargaining communities and may, in limited circumstances, designate the representatives of employees,[113]

---

111. The Raz elements relate to the existence and comprehensiveness of a legal system. *See* RAZ, *supra* note 32, at 1-2 (explaining that a complete theory of legal system seeks to solve four problems, including existence and membership). They are in a sense attributes of sovereignty. The jurisdictional models of prescription, adjudication, and enforcement are concerned with the scope of power of a sovereign, usually assuming that a sovereign exists. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 401 (1987) (describing three types of jurisdictions as "limitations" on state power in international law).

112. *See* Machinists Lodge 19 v. Soo Line R. Co., 850 F.2d 368, 375 (8th Cir. 1988) (stating general rule and noting exceptions).

113. *See, e.g.*, 29 U.S.C. § 159 (1994) (granting the National Labor Relations Board jurisdiction to define the bargaining unit); *see also* National Labor Relations Board v. Gissel Packing Co., 395 U.S. 575, 610-16 (1969) (describing situations in which a court may issue a bargaining order establishing the union as bargaining representative); Gourmet Foods, Inc. v. Warehouse Employees of St. Paul, 270 N.L.R.B. 578 (1984) (holding that the National Labor Relations Board does not have authority to establish a union as a bargaining representative when the union never had majority support within the bargaining unit).

these agencies neither define the rules governing the employment relationship[114] nor resolve individual disputes over terms and conditions of employment.[115] The Supreme Court has characterized a community covered by collective bargaining as a specialized community unto itself.[116]

Collective bargaining communities have a considerable immunity from state tort law.[117] The immunity is not absolute, and state law may be applied when it involves deeply rooted state interests.[118] The federal antitrust laws also give way to collective bargaining community decisions, as long as they are made within the traditional scope of workplace governance.[119]

Collective bargaining has normative rules expressed in collective bargaining agreements. Most collective bargaining agreements are comprehensive in this regard, including rules on every major subject of workplace governance, although they typically have "management rights clauses" allowing the employer considerable discretion to make specified entrepreneurial decisions. Collective bargaining has its own set of institutions—periodic negotiation for making rules and grievance arbitration for resolving disputes over rule application and enforcement. Collective bargaining has coercive mechanisms. It channels the

---

114. *See* National Labor Relations Board v. Insurance Agents Int'l Union, 361 U.S. 477, 486-88 (1960) (slowdown concurrent with labor negotiations does not constitute a refusal to bargain collectively; Congress intended that parties to collective bargaining have wide range of discretion).

115. *See* H.K. Porter Co. v. National Labor Relations Board, 397 U.S. 99,106-09 (1970) (holding that the National Labor Relations Board does not have the authority to compel the acceptance of any contractual provision in a collective bargaining agreement).

116. *See, e.g.*, United Steelworkers of America v. Warrior & Gulf Navigation Co., 363 U.S. 574, 579 (1960).

117. *See, e.g.*, San Diego Building Trades v. Garmon, 359 U.S. 236, 239-48 (1959) (holding state law against secondary pressure preempted); Lodge 76, Int'l Assoc. of Machinists and Aerospace Workers v. Wisconsin Employment Relations Comm'n, 427 U.S. 132, 144 (1976) (areas not addressed by federal law nevertheless are shielded from state regulation because Congress meant for them to be unregulated by law).

118. *See, e.g.*, Lingle v. Norge Div. of Magic Chef, 486 U.S. 399, 406-10 (1988) (public policy tort claim for wrongful dismissal is not preempted by federal enforcement of collective bargaining agreement covering employee when state claim is completely distinct).

119. *Compare* Brown v. Pro Football, Inc., 116 S. Ct. 2116, 2120-23 (1996) (nonstatutory antitrust exemption extended to unilateral imposition of compensation after impasse in bargaining), *with* Connell Construction Co. v. Plumbers Local 100, 421 U.S. 616, 626-35 (1975) (antitrust exemption did not extend to "pre-hire" agreement negotiated before any represented employees were in bargaining unit).

employer's power to discipline employees and terminate employment, and it organizes and channels the union's ability to put economic pressure on employers by striking. The union's strike weapon is less directly related to rule violation, although some collective agreements have exceptions to no-strike clauses that are triggered when employers violate rules set forth in the collective agreement.

Collective bargaining has all three Raz factors. The collective agreement institutionalizes workplace governance, it articulates norms, and it provides for coercive enforcement through strikes and termination of employment. As a model for network self-governance, collective bargaining is interesting because of its completeness and because of the limited immunities from antitrust and tort law enjoyed by its participants.

2. *MILITARY MODELS*

Military law governs military communities.[120] It is unique among the examples considered in this article because it goes the farthest in establishing immunities from the civil law of the traditional national community. Under United States military law, for example, a member of the armed forces is not subject to criminal or civil process for conduct associated with the performance of his duty. Military and naval communities historically have enjoyed such substantial immunity from the application of civilian law.[121] The immunity extends to military forces of both de facto and de jure governments.[122]

Nevertheless, members of military and naval forces are not completely immunized from civilian law. They may be charged with,

---

120. Membership in military societies is involuntary both because of the common historical practice of conscription, in which initial membership is involuntary, and because a member of the military establishment even if she was a volunteer at the outset is not free to terminate her membership unilaterally during its term.

121. *See* Underhill v. Hernandez, 65 F. 577, 581-83 (2d Cir. 1895) (reversing damages judgment against Venezuelan officer for harm done to an American citizen during revolution and reviewing cases establishing proposition that military officer enjoys sovereign immunity in international law).

122. A de facto government "exists where a portion of the inhabitants of a country have separated themselves from the parent state, and established an independent government. The validity of its acts, both against the parent state, and its citizens or subjects, depends entirely upon its ultimate success" Williams v. Druffy, 96 U.S. 176, 186 (1877).

arrested for, and tried for crimes committed within their forces.[123] Under some circumstances, writs of habeas corpus may issue to military authorities to show why a member of the military or naval force is detained.[124] Although damage actions are not allowed,[125] injunctions may issue for violations of civil rights.[126] Most of these cases involve internal military and naval disputes where the arguments against civil court intrusion are substantial. A fortiorari, members of otherwise autonomous military communities should be subjected to the surrounding legal system when the civil courts seek to adjudicate conduct in which a military authority injures a civilian.[127]

Military societies have normative rules for the conduct of individual members in the form of regulations and standing orders. They institutionalize rulemaking and enforcement through the chain of command and through rules defining the scope of the powers in each level of the chain of command, and they have courts marshal for dealing with rule violations. Military societies have coercive mechanisms that are employed directly against rule violators, including loss of pay, incarceration, and expulsion (discharge) from the service. They thus satisfy all three Raz criteria.

---

123. *See, e.g.*, United States v. Bevans, 16 U.S. (3 Wheat) 336, 386 (1918) (reversing conviction of marine sentry for murder committed aboard a ship of war because state courts had jurisdiction).

124. *See, e.g.*, Parisi v. Davidson, 405 U.S. 34, 35 (1972) (holding that habeas corpus may issue to inquire into basis for keeping conscientious objector in the service).

125. *See, e.g.*, Miller v. Newbauer, 862 F.2d 771, 774 (9th Cir. 1988) (well settled that no damages action may be pursued); Walden v. Bartlett, 840 F.2d 771, 773-74 (10th Cir. 1988) (affirming denial of damages but reversing denial of injunction for military prisoner alleging due process violations in connection with disciplinary proceedings); Knutson v. Wisconsin Air Nat'l Guard, 995 F.2d 765, 769-70 (7th Cir. 1993) (noting that there is some level of judicial review). *But see* Tigue v. Swain, 585 F.2d 909, 914 (8th Cir. 1978) (denying absolute immunity for alleged libel and false imprisonment by military officer).

126. *See, e.g., Walden*, 840 F.2d at 774-75 (reversing denial of injunction against military officials for alleged due process violations in connection with military disciplinary proceedings); *Knutson*, 995 F.2d at 770-71 (canvassing cases and concluding that no per se rule exempts military decisions from injunctive relief).

127. *See* B. ZOBEL, THE BOSTON MASSACRE 241-94 (1970) (describing the trial of British soldiers in regular civilian courts for "Boston massacre" resulting in the acquittal of most of them).

C. Voluntary membership models

1. *RELIGIOUS COMMUNITIES*

Religious communities long have enjoyed autonomy from secular sovereigns. In the United States, religious community autonomy is guaranteed by the free exercise clause of the First Amendment.[128] However, deference and immunity are limited to certain levels of subject matter. The deference relates only to matters of religious doctrine or policy, and to rulemaking and adjudication over internal discipline and government which has been interpreted to include "matters of discipline, faith, internal organization or ecclesiastical rule, custom, or law."[129] Other matters may be addressed with more or less autonomy pursuant to the contract rules applicable to other private associations.

Despite large measures of autonomy, traditional sovereigns impose boundaries on religious communities. Religious organizations may be liable for fraud for statements made outside the religious context[130] and for intentional infliction of emotional distress when they act coercively far beyond the bounds of customary religious practices.[131]

Religious communities can be complete Raz systems because they institutionalize, they articulate norms, and they coerce compliance by the prospect of expulsion from membership and from religious grace.

2. *PRIVATE ASSOCIATION MODELS*

Private associations like fraternities, churches, athletic leagues, country clubs, the Boy Scouts of America, and trade associations are largely self-governing, both with respect to rulemaking and adjudication.[132] One of the justifications for limited self-governance by private associations is freedom of association—a type of privacy interest.

---

128. *See* U.S. CONST. amend I.

129. Primate and Bishop's Synod of the Russian Orthodox Church Outside Russia v. Russian Orthodox Church of the Holy Resurrection, Inc., 617 N.E.2d 1031, 1033 (Mass. 1983) (describing a "neutral principles of law" analysis).

130. *See, e.g.*, Christofferson v. Church of Scientology of Portland, 644 P.2d 577, 598 (Or. 1982) (remanding for new trial, rejecting outrageous conduct liability because of voluntary nature of plaintiff's membership, and articulating rule limiting fraud liability to statements not involving religious matters).

131. *See, e.g.*, Wollersheim v. Church of Scientology, 66 Cal. Rptr. 2d 1, 6-18 (Cal. 1989) (affirming in material part judgment on jury verdict against religious organization).

132. *See* Note, *State Power And Discrimination By Private Clubs: First Amendment Protection For Nonexpressive Associations*, 104 HARV. L. REV. 1835, 1847 (1991) (articulating basic propositions).

The courts get involved only to enforce compliance with association rules.[133]

Private associations vary in the degree to which they have the three Raz attributes. Most private associations have normative rules, although their scope may be relatively narrow, limited to matters directly concerning the association rather than a broader range of human conduct. They have mechanisms for making rules to be recognized as such and usually have institutional arrangements for applying and enforcing rules. Coercive mechanisms in private associations usually are limited to expulsion, but some religious associations also subject rule violators to spiritual penalties or social penalties like shunning. Some non-religious associations like country clubs may subject rule violators to forfeiture of membership fees, which resemble a kind of security bond in this respect.

3. *CLEARINGHOUSE FUNCTIONS*

Clearinghouses handle the successive negotiation of checks and other financial instruments from the payee's bank to the drawee's bank, resulting in the eventual debiting of the drawer's account and crediting of the payee's account. Clearinghouses exist for electronic funds transfers and credit card transactions, as well as personal checks. The communication is mostly electronic, with paper instruments following later, if at all.

Bank clearinghouse functions are performed pursuant to clearinghouse bylaws and rules, which are contracts among participating banks. Although Article 4 of the Uniform Commercial Code supplies default rules for clearinghouse functions, these statutory rules routinely are altered by the clearinghouse rules.

Bank clearinghouses thus are examples of self-governing electronic communities. This example of self-governance is likely to be extended as electronic payment systems become more popular with buyers and sellers

---

133. *See, e.g.*, Rowland v. Union Hills Country Club, 757 P.2d 105, 108-09 (Ariz. 1988) (reversing summary judgment for country club officers because of factual question whether club followed bylaws in expelling members); Straub v. American Bowling Congress, 353 N.W.2d 11, 13 (Neb. 1984) (rule of judicial deference to private associations and compliance with association requirements, counseled affirmance of summary judgment against member of bowling league who complained his achievements were not recognized). *But see* Wells v. Mobile County Bd. of Realtors, Inc., 387 So. 2d 140, 142-45 (Ala. 1980) (claim of expulsion of realtor from private association was justiciable and bylaws, rules, and regulations requiring arbitration were void as against public policy; reversing declaratory judgment for defendant association).

of goods and services in cyberspace.[134] Nevertheless, there is nothing about the bank clearinghouse experience that suggests the extension of self-governance to persons or entities not actually signatories to the clearinghouse contract. Nor is there any indication that these communities are immune from rules developed by the surrounding legal system to address concerns of members of that larger community.

Financial clearinghouses have normative rules on the limited subject matter of allocating the risk of dishonor and setting time limits for the settlement functions in their financial communities. They have institutional mechanisms for applying the rules, although it is hard to find examples of clearinghouse agreements that provide for actual adjudicatory mechanisms for rule violations. Instead, the sanction for rule violation is to bear the loss. Enforcement takes the form of expulsion or bearing the loss.

4. *CORPORATION MODELS*

The corporation is an example of a private association that enjoys powers of self-governance, which may be enforced by traditional law, subject to certain limitations. In this respect, corporations are like the other private associations discussed above.[135] However, the corporate structure does offer advantages over other forms of business enterprises.

Of primary interest is the limited liability that the corporate form provides to its members.[136] Limited liability is premised upon the basic principles of agency.[137] In many instances, the principle will shield its agents from liability. For example, in certain circumstances, only the corporation, and not its agents, are liable on contracts made in the

---

134. *See generally* Henry H. Perritt, Jr., *Legal and Technological Infrastructures for Electronic Payment Systems*, 22 RUTGERS COMPUTER & TECH. L.J. 1 (1996).

135. Corporations have normative rules with respect to the allocation and commitment of corporate resources. They usually have rules relating to conduct in the workplace or on behalf of the corporation. They have institutions for rulemaking—usually the board of directors and a variety of management committees. They also may have formal institutional mechanisms for rule application and enforcement, although this also may be handled less formally through the managerial chain of command, with each supervisor applying and enforcing rules as to her subordinates. Coercion is limited to exclusion from the community, demotion, or repudiation of an action or decision.

136. *See* Stockmar v. Warrec Co., 844 F. Supp. 103 (D. Conn. 1994) (holding corporate officers not personally liable under state wage payment statute based on legislative intent).

137. *See generally* Restatement (Second) Agency (1958).

corporation's name.[138] However, there are other complex situations where the agent may be held personally liable. For example, the corporation and the agent, or both, may be liable for torts and crimes depending on the status of each party and the context in which such tort or crime occurred.[139] This may also affect "foreign" corporations (corporations incorporated in one state but doing business in another state), and thus must comply with certain formalities as defined by the other state's domestic law.[140] Absent compliance with these requirements, corporate actors may be found individually liable not only for torts and crimes, but also for contractual obligations into which they enter on the corporation's behalf. The same basic concepts for the treatment of foreign corporations apply internationally.[141]

The nature of limited liability for members of corporate communities is expressed by the legal fiction that a corporation is person. The corporation is treated as a separate legal entity,[142] which results in a

---

138. *See id* at §§ 140-43; HAROLD G. REUSCHLEIN & WILLIAM A. GREGORY, HANDBOOK ON THE LAW OF AGENCY § 118 at 182 (1979) (disclosing principal protects agent from liability).

139. *See id.* § 124 at 193-94 (acting for principal does not exculpate agent from tort liability). *See* United States v. Wise, 370 U.S. 405, 416 (1962) (reversing dismissal of Sherman Act indictment against individual corporate officer); *Compare* Bourgeois v. Commonwealth, 227 S.E.2d 714, 718-19 (Va. 1976) (holding corporate president not criminally liable for grand larceny absent proof he actually participated), *with* United States v. Dotterweich, 320 U.S. 277, 285-86 (1943) (upholding conviction of corporate president for criminal violations of Federal Food Drug and Cosmetic Act despite lack of proof of personal knowledge or participation).

140. *See* Gradison v. Ohio Oil Co., 156 N.E.2d 80, 83 (Ind. 1959) (construing state statute as granting qualifying foreign corporations all of the powers of domestic corporations); Cincinnati, Indianapolis & W.R.R. Co. v. Barrett, 94 N.E.2d 294, 296-97 (Ill. 1950) (holding foreign corporation that acquired domestic railroad not exempt from payment of registration fee merely because domestic railroad was exempt).

141. *See generally* LUCIE A. CARSWELL & XAVIER DE SARRAU, LAW & BUSINESS IN THE EUROPEAN SINGLE MARKET § 4.02 at 4-7 (1993) (explaining that liability is joint and several under European community law unless certain formalities are satisfied); *id.* § 4.03 at 4-11 (describing five formal requirements for the incorporation of a company); *id.* § 4.09[3] at 4-65 (describing European economic integrated grouping ("EEIG") as a kind of corporate joint venture operating across boundaries within the European community, but liabilities are joint and several thus negating much of the purpose). Inter-partner contracts purporting to limit liability are ineffective as against third parties for EEIGs. *Id.* at 4-70.

142. Acceptance of the concept that a corporation is an entity separate from its shareholders or members long antedates the development of limited liability for shareholders, which occurred in the middle of the nineteenth century in England, when law developed new structures to allow capital aggregation to exploit new technologies

tiered structure whereby management powers and limited liability may co-exist in a single individual in a corporation.[143] This legal fiction permits—at least in many instances—a third-party victim to be made whole through a legal claim against the corporation as an entity. The entity theory has received virtually universal legal acceptance, and the fictitious person so created has been given many of the constitutional protections available to individuals.[144]

The entity approach, however, has been subject to some criticism, especially in the context of the multinational enterprise. While in a strictly legal sense, a multinational enterprise can most simply be characterized as "an aggregate of corporate entities, each having its own juridical identity and national origin, but each in some way interconnected by a system of centralized management normally exercising its control from the seat of primary ownership," a multinational enterprise "has no coherent existence as a legal entity." [145] There is, however, a body of law emerging which is applicable to multinational corporations.[146] One such area consists of the rules of international law dealing with expropriation.[147] Nevertheless, efforts at establishing international codes and guidelines are relatively weak in their influence thus far, primarily because they are not legally binding.[148]

---

and larger markets made possible by new technologies. *See* P. Blumberg, The Law of Corporate Groups: Procedural Law 1-2 (1983).

143. Theoretically, a corporation consists of three tiers: (1) the shareholders who are traditionally viewed as the ultimate owners of the enterprise, (2) the board of directors, who are the managers of the corporation's affairs, and (3) the officers, who traditionally act as an officer, a director, and a shareholder. HAMILTON, CASES AND MATERIALS ON CORPORATIONS 9 (1994).

144. *See, e.g.*, Virginia Pharmacy Bd. v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748 (1976) (finding that a corporation has a First Amendment right to free speech); Helicopteros Nacionales de Columbia v. Hall, 466 U.S. 408 (1984) (holding a corporation is entitled to due process). Immunity in the contract and criminal areas is justified by two rationales: (1) the practicability of enforcement; and (2) the perception that corporate institutional liability is more likely to result in internalization of societal goals and the mobilization of corporate bureaucratic institutional mechanisms to enforce traditional legal standards.

145. CYNTHIA DAY WALLACE, LEGAL CONTROL OF THE MULTINATIONAL ENTERPRISE 2 (1982).

146. *See id.* at 3-4 (posing question of whether international regime of regulation of multinational corporations is desirable).

147. *See id.* at 249-294.

148. *See id.* at 300.

In the future, one area in which truly international corporations may emerge is in Europe. The European Union encourages member states to adopt domestic corporation laws that conform to standards set by a European Union directive. Thus, the company incorporating in one member state can do business in other member states without discrimination. It will be interesting to evaluate European Union mechanisms for incorporation to determine if a European Union corporation can achieve corporate status vis-à-vis member states without being separately incorporated in each member state.

5. *THE LAW MERCHANT*

The law merchant was a transnational private law based not on any single national law but on mercantile customs generally accepted by trading nations.[149] The law merchant (lex mercatoria)[150] originated in the pre-Christian era in the Mediterranean, spread through Europe in the Middle Ages, and was reinforced through Admiralty and Maritime law and through Roman and Canon law. Despite the influences of several bodies of law, business dealings "rested on mutual confidence and good faith to an extent unknown to civil life."[151] By the end of the eleventh century, the law merchant began to be formalized and incorporated into the codes of certain conventional governments.[152] Eventually, the law merchant was applied by the Admiral's Court in England and published in Italian, French, Latin, Dutch, and German as the "Consulato del Mare."[153]

More or less independently, a body of commercial law developed in so-called "fair courts." Annual fairs took place in various places on the continent of Europe, attracting traders from Africa, Russia, and the Middle East as well as Europe. Each fair had a dispute resolution body that heard commercial disputes among the participating merchants.

---

149. *See* Harold J. Berman & Colin Kaufman, *The Law of International Commercial Transactions (Lex Mercatoria)*, 19 HARV. INT'L L. J. 221, 224-29 (1978).

150. Lex mercatoria actually is a broader concept than the law merchant. Philip De Ly described lex mercatoria as consisting of "self regulatory rules of professional organizations, usages, customs, general conditions, usual contractual clauses and techniques, arbitration rules, arbitral case law, general principles of private law and general principles of conflict of laws." FILIP DE LY, INTERNATIONAL BUSINESS LAW AND LEX MERCATORIA 221 (1992)

151. W. BEWES, THE ROMANCE OF THE LAW MERCHANT 14 (1923).

152. *See* Mark Garavaglia, *In Search of the Proper Law in Transnational Commercial Disputes*, 12 N.Y.L. SCH. J. INT'L & COMP. L. 29, 34-35 (1991).

153. *See id.* at 35.

While the crown might appoint a judge to guide the proceedings, the juries consisted of merchants participating in that particular fair.[154]

By the late sixteenth and early seventeenth centuries, when national sovereigns began to encroach on the traditional law merchant, the law merchant governed a special class of people (merchants) in special places (fairs, markets, and seaports). It was distinct from local, feudal, royal, and ecclesiastical law. Its special characteristics were that (1) it was transnational; (2) its principal source was mercantile customs; (3) it was administered not by professional judges but by merchants themselves; (4) its procedure was speedy and informal; and (5) it stressed equity, in the medieval sense of fairness, as an overriding principle.[155]

Thereafter, certain factors led to the diminished importance of the law merchant as a separate legal system. These factors included the rise of nationalism, competition between different kinds of courts for legal business, the tendency of traders to settle down and conduct their affairs from a particular place rather than traveling from fair to fair, and the incorporation of certain substantive principles of the law merchant into municipal law.[156] Nevertheless, as Mark Garavaglia has explained, the law merchant survives in modern commercial law under the guidance of international arbitration, commercial arbitration, and the Uniform Commercial Code.[157]

Thus, until the seventeenth century, the law merchant was an independent legal system with its own normative rules, its own institutions, and its own coercive measures. After that time, it lost the latter two features but retained its own normative rules.[158] Nevertheless, Professor Philip De Ly has cautioned that modern international business

---

154. *See id.* at 36-39 (describing fair courts).

155. *Id.* at 33 n.10. *But see* DE LY, *supra note* 150, at 17-19 (expressing doubt on whether law merchant ever was completely separate from national legal systems).

156. *See* Garavaglia, *supra* note 152, at 38-39; *see* DE LY, *supra* note 148, at 17 (explaining that the substantive absorption of law merchant by common law dates to 1756 when Chief Justice Mansfield began to qualify trade custom as legal rules applicable to all citizens).

157. *See* Garavaglia, *supra* note 152, at 40-55, 79-102 (describing international arbitration, concepts of law merchant in American commercial law, the emphasis on trade usages and regular practices in Uniform Commercial Code, and American attitudes toward international commercial arbitration); Parsons & Whittemore Overseas Co. v. Societe Generale, 508 F.2d 969, 973-77 (2d Cir. 1974) (rejecting public policy challenge to international arbitration decision).

158. Mr. Garavaglia's work does not make it entirely clear whether the fair courts imposed their own sanctions or relied upon traditional legal institutions to enforce their judgments. See Garavaglia, *supra* note 152, at 36-38 (describing fair courts and state facilitation of fair court proceedings).

law is not really an autonomous legal system in the sense that it "exists outside national legal systems; rather within national systems, it has some features of its own," derived from international origins and leading to a uniformity of international business law.[159] Lex mercatoria does not have a monopoly on resolving transnational business disputes and may need national law to enforce decisions applying its rules. Yet, lex mercatoria is an independent body of law that can be applied by national courts under choice-of-law rules of contract provisions. Because of the tendency of national courts to apply their own law, international arbitration represents the best forum within which to apply and enhance the status of lex mercatoria as a complete legal system.[160] Of course, the content of lex mercatoria must be known in order for it to play an enhanced role. One way to achieve this is through the publication of arbitral awards.[161] One author described lex mercatoria as consisting of "self regulatory rules of professional organizations, usages, customs, general conditions, usual contractual clauses and techniques, arbitration rules, arbitral case law, general principles of private law and general principles of conflict of laws."[162] The distinction between reliance on these sources of law and proof of customs and usages is subtle.[163]

Lex mercatoria is significant not only as a model of community autonomy, but also as a legal doctrine that may legitimate recognition of electronic community "law," as explained in Part III of this article. This is so because it is the clearest example of satisfaction of the four criteria that justify self-governance for electronic communities.[164] Lex mercatoria, however is not a complete Razian system because it lacks its own institutions and coercive measures.

D. Conclusion

All of the models exhibit some degree of autonomy because traditional sovereigns defer to them. All of the models, except lex mercatoria, are relatively complete Razian systems because all institutionalize their internal law, develop their own norms, and employ coercive enforcement power through expulsion from membership. Collective bargaining and military models have stronger coercive

---

159. DE LY, *supra* note 150, at 209-10 (1992).

160. *See id.* at 16.

161. *See id.* at 225.

162. *Id.* at 221.

163. *See id.* (describing how usages must be proven, while customs as rules of law may not need to be proven).

164. *See supra* Part III.

enforcement tools like the strike and direct physical action against military members. Corporations are less complete Razian systems because they employ coercive measures only against some constituents.

The frameworks for self-governance in all but the military communities are contractual. Antitrust and tort immunities are recognized by traditional sovereigns for many of the communities. Autonomy has its limits, however, in every model. Certain means and purposes justify application of traditional law, overriding the autonomy otherwise enjoyed by the community.

Aspects of all of these examples provide exemplars for electronic communities. Their utility depends, however, on working out institutional details for electronic counterparts and on developing appropriate immunities to define the boundary between electronic communities and traditional legal systems.

VII. WHAT REMAINS TO BE DONE?

Self-governance for electronic network communities is desirable: it is legally feasible within a contractual framework; examples already exist in parts of cyberspace; and rich models exist in the form of other types of private associations and communities. Establishment of comprehensive systems of self-governance for the Internet requires fleshing out contractual webs, defining antitrust and tort immunities according to established doctrine and newly articulated criteria for autonomy, and eventual development of a treaty framework.

A. Completing the contractual web

1. DEVELOPING NORMS FOR ELECTRONIC COMMUNITIES

The section on the legal feasibility of self-governance observed that completeness enhances deference by traditional legal institutions. Complete legal systems include rulemaking, adjudication, and enforcement. Earlier sections explained how adjudication can be provided through arbitration, and how denial of access to net resources—through the domain registry—can provide enforcement. That leaves rulemaking as the most significant challenge for developers of a comprehensive contractual web for self-governance.

Self-governing communities must have institutions to serve as sources of law. Institutions in cyberspace for rulemaking would exist on top of and in parallel with geographic-based institutions like state and federal courts and international rulemaking and adjudicatory institutions.

One possibility is to establish an electronic structure for a continuing plebiscite, such as that represented by a.c.e.n.a.[165] Alternatively, and more formally, electronic communities could identify a dozen or fewer experts in the norms and values of conduct in cyberspace to be rule-makers.[166] The IAHC recommendation includes such a mechanism in its policy committee.[167] In other contexts, the lawmakers need not be members of the community.

These "wise men and women" might function like the American Law Institute, publishing a restatement of appropriate principles to guide conduct in cyberspace. They also might function as arbitrators.[168] They also might play ancillary roles like being called as expert witnesses by the regular courts presented with cyberspace disputes. There is no reason that a single panel of experts cannot serve multiple communities as the lawmakers for those communities. The concept is roughly like a state adopting a particular section of a restatement written by the American Law Institute. The state, acting through its legislature or courts, reaches outside its own institutions to incorporate a doctrine developed for use by multiple communities.

More formally, one can follow other aspects of the model suggested by the IAHC, and write a kind of constitution that builds representative rulemaking institutions in a hierarchy defined by the domain name registration system for the Internet. The limitations of this model relate to the fluidity of "citizenship"—the composition of constituencies—at lower levels of the hierarchy.

2. *DEFINING MEMBERSHIP AND BOUNDARIES*

One of the greatest difficulties in formulating a means for electronic community self-governance is the difficulty in defining the boundaries of that community. The most fruitful source of guidance for defining a self-governing community is contract law. Determining the class of parties to the contract defines the boundaries of the community. The issue often arises when an individual files a lawsuit to compel arbitration or a community member might file a motion to dismiss a lawsuit for failure to exhaust arbitration remedies because a community may choose

---

165. *See supra* Part V.A-B.

166. The same individuals chosen to be rule-makers also could be dispute resolvers.

167. *See supra* notes 72-96 and accompanying text.

168. Arbitration is usually thought of as an adjudicatory mechanism that applies preexisting rules. However, there is no bright-line between rulemaking and adjudication in the common law tradition. Arbitrators and common law tradition can make law by elaborating and extending basic principles.

arbitration as the first step in its self-governance scheme. A court hearing either type of suit must decide if the reluctant party has agreed to arbitration. Only parties to the arbitration agreement are bound to arbitrate.

One can draft an arbitration agreement that represents a multilateral contract among all the members of a community, but the agreement will not effect individuals outside the community. Most existing models for self-governance present situations in which there is little doubt who is a member of the community, and thus little doubt as to the boundaries of the community's powers of self-government. For instance, nation-states are geographically defined, and international law places great emphasis on geographic boundaries in determining the reach of sovereignty. Further, the involuntary models, collective bargaining and military societies, have formal rules for determining who is a member of the community: induction and swearing in the case of military institutions and definition of an appropriate bargaining unit or craft or class in the case of collective bargaining. Finally, in the voluntary models, including private associations and bank clearinghouses, the act of joining and submitting to the rules of the private community defines the membership.

Electronic communities do not ordinarily have geographic boundaries, and thus that technique for defining membership and the boundaries of governance is unavailable. Furthermore, it is unlikely that traditional legal systems will provide formal rules to define membership along the pattern of the collective bargaining model or the military model until electronic community self-governance has been a reality for a considerable period of time.[169] The private association and clearinghouse models, which focus on a voluntary act of joining, appear to provide the best starting point for analysis of electronic community formation.

There may be problems in adapting conventional tests for contract formation to some electronic communities. While the act of subscription to America Online, CompuServe, or Lexis Counsel Connect may be unambiguous, it is not clear what the relevant act is in "joining" an Internet newsgroup or a community whose activities are carried on through Web-based postings. Does one "join" and thereby become subject to the rules of that newsgroup simply by reading the back postings from a newsgroup on one occasion, or by clicking into a Web site? If so, for what period of time is one member subject to that community's rules? Perhaps, only when one is reading and posting. This

169. Compelling submission to private governance may be politically unpalatable until there is more empirical evidence of the desirability of such compulsion.

answer satisfies the specialization justification for autonomy.[170] However, the transitory nature of membership in this example defeats almost any conceivable sanctioning power that the community could have. The sanction would only be effective if the community's resources are so attractive that exclusion is effective.

Notwithstanding the previous discussion, one should not overplay the importance of precise community membership definition. One can generally define boundaries in relation to the practical nature of the community. Even traditional national states have variable membership. As new people become citizens, others renounce their citizenship, and aliens come and go, sometimes these individuals fall within the power of the state and sometimes not. Moreover, nation-states have mechanisms for bringing ex-members within their communities again forcibly, such as extradition and reciprocal enforcement. Similarly, in the collective bargaining context, the class of employees covered by a collective agreement changes constantly as new persons are hired, and existing employees retire or are terminated. While all communities must define some reasonably ascertainable boundaries, these boundaries are defined in relation to the practical nature of the community. It might be quite feasible to define membership in certain electronic communities as the traffic moving through the community facilities at any given time.

The risk of sweeping significant numbers of people under the jurisdiction of private legal institutions to which they have not consented in fact, and with which they may be unfamiliar, will exert pressure on traditional legal institutions—legislatures, courts, and agencies—to draw narrower boundaries. When plausible boundaries, albeit fuzzy ones, are definable, then the arbitration mechanism can interpret those boundaries in particular cases.

3. *LEGALIZING*[171] *COERCIVE ENFORCEMENT OF COMMUNITY RULES*

There are two mechanisms for autonomous enforcement of community decisions: (1) execution against some asset made available as a security, such as a bond posted by member of a networked community or intellectual property left within the community; and (2) expulsion or exclusion from the community. The first of these mechanisms is available only if the network community requires the posting of some security as a precondition for membership. It might be feasible to require providers of

---

170. *See supra* Part III.B.

171. As I use the term, "legalizing" signifies recognizing privileges or immunities for self-governing activities that otherwise would produce liability in traditional legal institutions.

services to become members and post security before they are entitled to use network resources, like routers and network access points. Network communities might also require consumers to provide authorization to charge a credit card in advance. The limitation of this approach to enforcement, however, is that public key encryption[172] will permit a large volume of very small commercial transactions on open networks. In this context, consumers are unlikely to give authorization for enforcement security. Internet domain names present the most interesting possibility for an appropriate property interest. As discussed above, the IAHC proposal for privatizing and internationalizing domain name assignment and registration[173] shows how such a property interest might be the focus of coercive enforcement.

The second approach is to exclude community members who break the rules. Exclusion or expulsion is the most effective means of coercive enforcement of community norms. It is found in all the models for self-governance discussed above, except for lex mercatoria.[174] When social or economic resources available only through membership are valuable and more or less unique, the threat of exclusion provides a powerful incentive for rule compliance. Although the availability of competitive alternatives reduces the likelihood of antitrust liability for exclusion,[175] these same alternatives reduce the effect of exclusion as an enforcement technique. If a rule violator can just as easily go to another node on the Internet or to another service provider and get the same thing, exclusion is not very coercive. Nevertheless, the members of the network community may not focus on whether exclusion inflicts significant injury on the violator. Rather, they may seek to keep him out of that community and thus eliminate the possibility of his causing further injury within the community.

Effective enforcement of electronic community norms is easier when the community has reasonable solidarity. Solidarity is characterized by several important preconditions to informal community governance. Most important among these are the likelihood of continuing relationships among the people making, enforcing, and violating the rules as well as the existence of multidimensional relationships in the

---

172. *See supra* note 12.

173. Revocation of a domain name is an effective means for expelling someone from the Internet. Accordingly the IAHC report provides for effective enforcement—at least if solidarity can be maintained. *See supra* notes 72-96 and accompanying text.

174. *See supra* Part VI.

175. *See infra* Part VII.B.

community.[176] While the first of these prerequisites may be met in electronic communities, the second usually is not. Participants in electronic network communities may have continuing relationships, but their relationship is unidimensional; it involves only a particular type of communication and none of the other important human activities. This unidimensionality greatly weakens the force of informal community sanctions, such as social disapprobation by other members of the community and ultimately expulsion from the community.[177] If a violator of network community norms gets expelled, he simply can connect to another network. At least, he can do this if the market structure is competitive.

B. Immunities and community boundaries

Vigorous self-governance in cyberspace will involve conduct that ordinarily could give rise to liability imposed by traditional sovereign institutions. In particular, antitrust liability may result from rulemaking involving competitors and tort liability may result from accusations and testimony in adjudicatory proceedings. Robust self-governance depends on recognition of appropriate antitrust and tort immunities, as are already enjoyed by other self-governing communities.[178] Their availability to electronic communities usefully may be conditioned on certain criteria sketched out in an October 8, 1997 meeting in Washington, DC, presided over by this author, described in the Appendix, *infra*.

---

176. Multidimensionality is not fully explanatory. For example, stock exchanges are communities that surely are unidimensional in the modern world. Nevertheless, they exercise a good degree of self-government. This fact can be explained within the basic model by observing that when a single dimension has great importance to the members of a community, it can dominate other dimensions that tie the member to other communities. Alternatively, one can reason that an extremely important single dimension (like the economic interests of a broker in her membership in a stock exchange) spills over into other dimensions: A broker expelled from a stock exchange may be unable to send her children to college and may lose her spouse, thus implicating social, familial, and other noneconomic dimensions.

177. *See* Perritt, *Community Regained*, *supra* note 7, at 1009.

178. *See infra* Part IV.B.1-2.

1. *IMPOSING SANCTIONS WITHOUT VIOLATING THE ANTITRUST LAWS*[179]

As detailed in the preceding sections, contract law provides a promising framework for the proscriptive and most of the institutional prerequisites to a complete legal system for electronic communities. However, contract law may fail to provide any effective coercive sanctions for rule violators. The most likely sanction for violating electronic community rules is exclusion from the community. The problem is that the contract providing for exclusion—or providing the mechanisms through which exclusion is imposed—potentially runs afoul of the Sherman Act.[180] A contract providing for exclusion from the community is a restraint of trade within the meaning of the Sherman Act and, depending upon the specific facts and circumstances, may be categorized as either a "concerted refusal to deal" or an "exclusive dealing arrangement." A concerted refusal to deal arises when two or more persons agree not to deal with a third party.[181] An exclusive dealing arrangement arises when a buyer agrees to purchase all of its requirements from a particular seller.[182] Although excluding a member

---

179. A thorough analysis of the antitrust implications of Internet self-governance is beyond the scope of this paper. This paper will briefly outline the major considerations. For a more complete analysis, *see generally* PERRITT, INFORMATION SUPERHIGHWAY, *supra* note 12. Of course, antitrust laws differ among countries around the world. While the basic rules are similar to those applied in the United States, the details vary considerably. Because of the similarities in the laws, this discussion will focus on the antitrust laws of the United States. However, it is important to note that the self-governance of electronic communities must be effective globally. Ultimately, an international agreement may be necessary to give requisite certainty. In order to be effective, this international agreement should be self-executing so that legislative implementation by state parliaments is not necessary.

180. Section 1 of the Sherman Act declares that "[e]very contract, combination in the form of trust or otherwise, or conspiracy in restraint of trade or commerce among the several States, or with foreign nations, is hereby declared to be illegal." 15 U.S.C. § 1 (1994).

181. *See, e.g.*, Eastern States Retail Lumber Dealers' Ass'n v. United States, 234 U.S. 600, 606-14 (1914); Klor's, Inc. v. Broadway-Hale Stores, Inc., 359 U.S. 207, 209-14 (1959).

182. *See, e.g.*, Standard Oil Co. v. United States, 337 U.S. 293 (1949); Tampa Electric Co. v. Nashville Coal Co., 365 U.S. 320 (1961). Exclusive dealing arrangements may also violate section 3 of the Clayton Act. *See* 15 U.S.C. § 14 (1994). However, the Clayton Act only applies to the sale of goods. Moreover, exclusive dealing arrangements may violate section 5 of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(a)(1) (1994) (declaring

from the community is a restraint of trade, it only violates the Sherman Act if the restraint is unreasonable.

Most restraints are judged under a rule of reason analysis in which the anticompetitive effects of the restraint are weighed against the procompetitive effects.[183] However, this rule of reason analysis entails a fact-intensive inquiry that produces significant societal costs in terms of business certainty and litigation efficiency.[184] Therefore, "there are certain agreements or practices which because of their pernicious effect on competition and lack of any redeeming virtue are conclusively presumed to be unreasonable and therefore illegal without elaborate inquiry as to the precise harm they have caused or the business excuse for their use."[185] This is a per se antitrust analysis. Exclusive dealing arrangements are evaluated under the rule of reason analysis.[186] However, the per se analysis is applied to certain concerted refusals to deal.[187]

Nonetheless, "not every cooperative activity involving a restraint or exclusion will share with the per se [concerted refusals to deal] the likelihood of predominantly anticompetitive consequences."[188] The per se approach is most often utilized when there are joint efforts to disadvantage competitors by denying relationships that the competitors need in the competitive struggle, the dominant parties have market power, and the practices are not justified by any plausible arguments that they were intended to enhance overall efficiency.[189] In cyberspace, there is no anticompetitive effect when the person excluded is not a producer. However, in other situations, the excluded individual may be a producer. For example, a packet routing consortium may decline to handle packets

---

unlawful, any "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.").

183. In making this determination, courts consider a number of factors including the natural and probable consequences of the restraint, the history of the restraint, the evil believed to exist, the purpose of the restraint, the market power of the participants, and any other less restrictive alternatives. *See, e.g.*, Chicago Board of Trade v. United States, 246 U.S. 231, 238-39 (1918); National Collegiate Athletic Ass'n v. Board of Regents, 468 U.S. 85, 104-13 (1984).

184. *See, e.g.*, Northern Pacific Railway v. United States, 356 U.S. 1, 5 (1958); Northwest Wholesale Stationers, Inc. v. Pacific Stationery & Printing Co, 472 U.S. 284, 289 (1985).

185. *Northern Pacific*, 356 U.S. at 5.

186. *See e.g.*, Bar. Lab., Inc. v. Abbott Lab., 978 F.2d 98, 110 (3d Cir. 1992).

187. *See, e.g.*, Eastern States Retail Lumber Dealers' Ass'n v. United States, 234 U.S. 600, 606-14 (1914); Klor's, Inc. v. Broadway-Hale Stores, Inc., 359 U.S. 207, 209-14 (1959).

188. *Northwest Wholesale Stationers*, 472 U.S. at 295.

189. *See id.* at 294.

belonging to a network service that fails to apply the rules agreed upon by the consortium. In these circumstances, the bodies of self-governance must be prepared to explain how the sanction of exclusion enhances competition.

Health Care Peer Review[190] is a particularly pertinent area of antitrust analysis of self-governance[191] because health care peer review, like cyberspace adjudication and enforcement is a form of specialized self-government. The result of peer review often is exclusion from a particular facility or specialty, just as the result of cyberspace adjudication may be exclusion from all or parts of cyberspace.[192] "Although revocation of doctor's privileges may, perforce, eliminate competition by decreasing the number of doctors in a given specialty, this alone will not give rise to an antitrust violation."[193] An essential element of a section 1 violation is proof of an unlawful objective, and "[c]orrective action against a physician does not violate the antitrust laws if the physician's peer reviewers had legitimate medical reasons to believe that the physician provided substandard care." That is so because monitoring the competence of physicians through peer review is clearly in the public interest.[194] Actual support for the peer review decision enters into the analysis because if "the peer group's conclusions are so baseless that no reasonable medical practitioner could have reached those conclusions

---

190. Health care peer review is a system through which health care professionals, usually physicians, review the conduct of another member of their profession to determine if it satisfies the applicable norms of practice. When the answer is "no," the result often is exclusion from practice in a particular facility such as a hospital or expulsion from the profession altogether.

191. Other examples of antitrust immunity for self-governing communities are considered in the review of models for self-governance outside the cyberspace context. *See supra* Part VI.

192. The dimensions of the antitrust liability of Health Care Peer Reviews have been altered by Congress' enactment of the Federal Health Care Quality Improvement Act, 42 U.S.C. § 11112 *et seq.* (1994), which immunizes from antitrust liability peer review actions meeting certain criteria: being based on a reasonable belief that the action furthered quality health care, appropriate fact gathering, notice and hearing, and reasonable belief resulting from the fact gathering and hearing that the action taken was warranted. The health care peer review act requires the opportunity for a hearing either before an arbitrator or before a hearing officer or panel not in direct competition with the involved physician. *See* 42 U.S.C. § 11112(b)(3)(A)(iii) (1994). The federal act permits states to opt in or opt out. However, even before the enactment of the new legislation, not all Health Care Peer Reviews were subject to antitrust liability.

193. Willman v. Heartland Hosp. East, 34 F.3d 605, 610 (8th Cir. 1994).

194. *See id.* at 610-611.

after reviewing the same set of facts," a fact finder may infer the existence of an illegitimate motive.[195]

Generally, antitrust scrutiny of competitive collaboration to impose and enforce rules should focus on whether any restraints on competition are (1) ancillary, that is truly necessary for legitimate purposes, and (2) crafted to minimize the risk of anticompetitive effects.[196] On the other hand, restrictions on competition cannot be defended successfully by mere claims that they are inspired by pure or public spirited motives; instead, the actions must be justified as not incompatible with maintenance of effective competition.[197] "Coercive boycotts" of unapproved providers are "almost certainly unlawful regardless of their arguably worthy purpose," and that antitrust immunity depends on the peer review organization simply making a report to others like public licensing authorities, hospitals, insurers, referring physicians, and patients themselves who decide for themselves whether to act on the advice provided by the peer reviewers.[198]

The case law and commentary on physician peer review is directly applicable to "peer review" by competitors in cyberspace. The public policy in favor of self-regulation of cyberspace is similar to the public policy in favor of self-regulation in the medical profession. Market structures are similar, and the utility of due process in deflecting claims of anti-competitive motivations is the same in both industries. The crucial question is whether public policy is stronger in the case of physician self-regulation because it is useful to go beyond the external standards, and because it is clear to everyone that physicians have a profession that outsiders are hard-pressed to analyze. Advocates of similar treatment for cyberspace must show how the criteria for autonomy[199] are satisfied as strongly for cyberspace as for medicine. They probably are. Specialized rules and adjudication are needed as much for cyberspace as for medicine. Traditional communities are probably more indifferent to the content of most cyberspace rules than to most medical practitioner rules because the latter are almost all likely to have effects on nonmembers of the medical professions. The inherent likelihood that a specialized legal system will be more efficient, that it will induce greater voluntary compliance, and that it will regulate

---

195. *See id.* at 611.

196. *See* Clark C. Havighurst, *Professional Peer Review and the Antitrust Laws*, 36 CASE W. RES. L. REV. 1117, 1119 (1986).

197. *See id.* at 1120.

198. *See id.* at 1129.

199. *See supra* Part III.

behavior that otherwise would escape regulation tilt the political balance in favor of autonomy in both areas.

In order to facilitate Internet self-governance, it is important to formulate a more extensive antitrust immunity. First, proof of an anticompetitive purpose that is not legitimated by some plausible need for standardization would defeat the immunity: only those decisions that could be related to a legitimate private government objective would be within the revised immunity. Private governance regimes such as those proposed by the IAHC clearly have a purpose other than restricting competition; indeed they were developed for the purposes of increasing competition in the market for domain name administration services. Second, due process should accompany both rulemaking and adjudicatory and enforcement decisions. Assuring due process would militating in favor of accountability, access to decision-makers, and rationality of decision-making.

2. *TORT IMMUNITY*

Also important is the availability of a tort privilege or immunity so that accusations and findings of fact can be communicated without giving rise to liability for defamation. The present formulation of privilege in the Restatement (Second) of Torts[200] appears to be broad enough to afford the requisite tort privilege. Because the common law is uncertain, however, and because the Restatement only purports to synthesize American common law, it would be desirable ultimately to express the tort privilege in an international agreement that articulates the competition-law immunity.

There also are potential problems with contractual liability when entities covered by the IAHC machinery implement decisions to exclude malefactors. The IAHC machinery cannot be implemented without standardizing contracts of service through the full range of Internet Service Providers. Such standardized contracts not only should present the arbitration alternative for domain name disputes; they also should wave any liability for breach of contract for the enforcement of decisions reached through arbitration.

---

200. *See* RESTATEMENT (SECOND) OF TORTS, §§ 585-590 (absolute privilege to make accusations as a part of legal proceedings). *See generally* PERRITT, INFORMATION SUPERHIGHWAY, *supra* note 12 (discussing tort privileges).

3. *RECONCILING "CONVERSATIONAL" MODES OF GOVERNANCE WITH DUE PROCESS*

The possibility of self-governance in electronic communities is a particularization of a broader set of issues arising from the growing use of digital technologies to conduct social, commercial, and political relations. Many commentators have observed that the growing use of such technologies tends to make human interaction more fluid—more conversational—and to erode formalities. There are, however, important questions presented if this assessment is correct.[201] Then one must address the tension between conversational modes of decision-making and the legal role of formalities. Conversational modes of decision-making may be antithetical to the kind of due process necessary to assure antitrust immunity.

Legal formalities such as signature and writing requirements and witness and attestation requirements in the law of contracts and wills serve three functions: cautionary, evidentiary, and channeling.[202] As digital technologies reduce formality, one must ask whether the need for these functions has been reduced, or whether the need still exists, but they can be performed in other ways with new technologies.

A tension exists between informal decision-making in electronic community self-governance on the one hand and the concepts of procedural due process on the other. As a particular example, if government decision-making becomes a kind of ongoing conversation instead of being manifested in discrete decisional documents like final rules, statutes, and judicial decisions, one must question whether the traditional procedural due process requirement that one have notice of a rule that one is obligated to obey is present. The only way one has notice of the current version of the rule is to participate continuously in the conversation over it. Even if one participates, there is no certainty that the rules will be the same next week as it is today. This kind of uncertainty traditionally is viewed with alarm by advocates of the rule of law.

---

201. It also may be questioned whether the use of digital technologies does tend to make things less formal and more fluid. It may be that the increased scope of participation made possible by digital technologies will increase formality as a means of coping with the disorder and anarchy that otherwise would result.

202. *See generally* PERRITT, INFORMATION SUPERHIGHWAY, *supra* note 12 (explaining purposes of formalities in contracting).

C. International treaty

Given the need for tort and antitrust immunity, as well as the need to recognize private government institutions, the regular states of the world should negotiate an international understanding that implements the principles the Clinton Administration and the European Union announced in July 1997.[203] This legal framework would set the ground rules for private Internet governance in terms of transparency, opportunities to participate, and other due process issues in rulemaking, adjudication, and enforcement. When the private institutions reach decisions under these criteria, signatory states would obligate themselves to respect those decisions. The framework document need not specify in any detail what "respect" means. Any action taken within the appropriate governance mechanism that satisfies the criteria would be immune from antitrust and tort liability under international and national law.

The multilateral international framework also should reduce uncertainty by specifically empowering certain existing multilateral institutions (such as the World Intellectual Property Organization, the International Telecommunications Union, and the World Trade Organization) with certain ministerial powers to support the private Internet governance institutions. Of the existing multilateral organizations, the World Trade Organization is especially desirable because of its commitment to open competition and its recent negotiation of a telecommunications agreement.

VIII. CONCLUSION

Computer networking technologies enable new communities to arise that are not limited by traditional boundaries of time and geography. Some of these new communities may be strong enough or sufficiently specialized that they seek autonomy from surrounding legal institutions. A variety of models for relatively autonomous, self-governing communities exist, and contract law provides the mechanism for beginning the process of self-governance. An international arbitration agreement is a particularly strong mechanism for defining self-governance across international boundaries. Ultimately, however, certain kinds of disputes between community members and outsiders will remain within the jurisdiction of traditional rulemaking and adjudicatory institutions.

The Internet functions through bits and bytes being routed through the Internet protocol to autonomous nodes and networks throughout the

---

203. *See supra* note 1 and accompanying text.

world. Thus understood, the Internet is a prime candidate for self-regulation and private governance. But the Internet also functions through real people, corporations, and non-profit organizations. It functions through hardware, software, and communications channels owned by real people and organizations. Those people, organizations, and their tangible property are currently, and will remain for the foreseeable future, subject to outside legal institutions. Unless appropriate steps are taken to harmonize regular law with new forms of private Internet self-governance, self-governance of the Internet will be frustrated when more than 200 legislatures and thousands of administrative agencies around the world develop their own rules. People will second-guess the decisions of expert Internet adjudicatory bodies. Further, losing parties in the self-governance institutions will ignore decisions they do not like because they need not fear enforcement from the regular police and army. DNS servers, routers, firewalls, and web servers that comply with the private regulatory regime, nevertheless, will be punished and put out of business for failing to comply with traditional law.

This is not a positive scenario. Policy-makers can prevent it only if they by take action designed to develop a comprehensive contractual framework for self-governance. This development should draw particularly on the foundation suggested by the IAHC. Traditional sovereigns should shield it with an over-arching treaty framework of forbearance to assure adequate breathing room to new private self-governance within the Internet.

Regardless of the particular aspects of self-governance that might apply, the concept of self-governance is not helpful unless some electronic communities proceed to take the first few steps. Those steps involve the development of principles, codes of good practice, and even stronger forms of rules. The community should develop them through conventional contractual mechanisms, and actually apply them through some form of arbitration or contractual fact-finding. If an electronic community cannot get this far with self-governance, it will not get further; nor will traditional legal systems accord it the deference or immunity it desires.

Self-governance for the Internet is desirable for several reasons: self-governance may be more efficient; electronic network communities need different rules and procedures; open networks escape enforcement of conventional rules; and self-governance promotes voluntary compliance. Self-governance for the Internet is legally feasible within contractual frameworks and already exists in certain parts of cyberspace. These contractual models, properly supplemented by aspects of other models for private autonomous communities, will provide a complete system for private rulemaking, adjudication, and coercive enforcement of

community decisions. Antitrust and tort immunity is necessary to permit such a system to function effectively. Fortunately, there is much precedent for such immunities, and they can be limited by criteria for open participation, due process, and protection for traditional norms.

IX. APPENDIX: CRITERIA FOR AUTONOMY

On October 8, 1997, a number of Internet stakeholders met in Washington to define the boundary between Internet self-governance and the governments of sovereign countries. This author convened the meeting in response to declarations by the United States and European governments that called for private sector leadership and self-regulation of the Internet. Participants recognized that no system of self-governance can exist independently of national systems of law and that the degree of connection between private regulatory bodies and traditional legal institutions varies by issue. In any system of self-regulation, it is necessary to ask what can be done to heighten confidence that a particular issue will be handled in a way that will be fair, legitimate, and efficient.

Self-regulatory systems meeting certain criteria can inspire that confidence. The participants in the October 8th meeting reached agreement in principle on five such criteria, which are set forth below. The strength of agreement was greater for the first three criteria than the fourth and fifth, and greater on the text of each criterion than on the explanatory notes that follow the statement of each criterion. The explanatory notes are examples and limitations to explain the intended operation of the criteria. Not every participant on October 8th agreed with every word of the principles and the explanatory notes, but the following statement fairly reflects the judgment of the group taken as a whole.

These criteria are intended for use by the designers of self-regulatory systems, by government policy-makers, and by judges who must determine the degree of deference to accord the decisions of private self-regulatory bodies for the Internet. When a self-regulatory system meets all the criteria, its private decisions made consistent with its constitutional documents are entitled to judicial deference and to some insulation from antitrust and tort law.

A. Any private system of Internet domain name administration and any other aspects of self-regulation must be transparent.

Explanatory notes:

- Rules and agreements should be disseminated and published widely on the Net, in an understandable and complete form.
- The process for amending and setting rules should be fully disclosed.
- Rules should be able to be created and changed only after an adequate notice period.

- Initiation and results of adjudications should be fully disclosed, including the factual and legal basis for the decision.
- Enforcement procedures and decisions should be fully disclosed.
- Who is making decisions and how they were selected should be publicly disclosed.

B. Rule making and adjudication within a private governance body must provide due process.

Explanatory notes:

- Decisions should be expressed in writing (including electronic formats).
- Adjudicatory decisions should be preceded by some form of hearing appropriate to the factual issues, and to the magnitude of the interests at stake.
- Decisions on rules and adjudications should be preceded by notice.
- Review of self-government decisions should be available, but should be confined to whether due process was made available not to the correctness of the decision on the merits; exceptions to this limitation on review should be reserved to cases implicating the protective principle below.

C. The actions of a private system of Internet domain name administration must be accountable.

Explanatory notes:

- The market provides a substantial degree of accountability, insofar as registrants may choose freely (in a free market) among a number of different registrars and registries offering diverse terms, conditions and policies.
- Additional accountability stems from the felt duty of all industry providers to assure that the net continues to work smoothly.
- Policy-making should be centralized only for issues as to which there is a need for a single, central rule, such as the policy of concurrence or interoperation.
- Each registrar is accountable to registrants according to the terms of the registration contract, and vice versa, provided that the registrar does not engage in fraud.
- Countries may or may not choose to require that actions within a country code comply with, and are thus accountable to, the law or policy established by that local government. In

any event, the relationship between any particular country code domain and the law or institutions of a particular country should be disclosed to registrants, who should be free to decide whether or not to contract to register within such domains.

- Registries, which set policies for any particular domain and the corresponding set of registrars, should promise each other that they will enforce their own stated policies, and should be accountable to each other for doing so.
- Registries, individually and in groups, should appoint or elect appropriate bodies to resolve disputes and make rules with respect to registrations within their domains.
- One or more new entities, constituted as membership organizations or non-profit corporate entities (perhaps with multiple classes of stock), membership in (or ownership of) which is open to all in exchange for appropriate fees, should establish or oversee policies for various domains.
- Entities governing particular domains may appoint or elect a centralized entity to coordinate their actions and/or play the centralized roles previously performed by IANA.
- The decisions of such domain policy setting entities should be entitled to deference by local courts under doctrines similar to the business judgment rule, and under the criteria expressed in this document.
- Insofar as the officers or trustees of entities exercising policy oversight over domains are elected on the basis of membership or stock ownership, individual persons or corporations should not be allowed to accumulate or vote multiple or duplicative memberships or ownership interests. Such memberships or stock interests may have multiple classes, reflecting appropriately the relative economic stake or representative reach of the institutions eligible to hold such classes of membership or stock.

D. An open opportunity must exist for anyone meeting stated qualifications to participate.

Explanatory notes:

- Openness must operate on four levels:
  - Cooperative agreements among sovereigns (treaties).
  - Composition and deployment of policy oversight entity.
  - Freedom of entry among registrars (multiple business models).
  - Consumer choice (portability and variety).

- Freedom of entry for registries should be tempered by:
  - Assurances of continuous and accurate resolution of domain name requests by way of a shared database.
  - Insurance against private failure leading to collapse of system by way of surety bonds and maintenance of "slave" servers.
- ISP's should subsidize the root server infrastructure.

E. Acceptable criteria must exist to avoid contract overreaching and for intellectual property protection and protection of the interests of third parties.

Explanatory notes:

- Inter-registrar agreements should recognize intellectual property rights
- There must be some recourse to national sovereignty.
- Dispute policy must come from a source other than registrars.
- It may be desirable for all registrars to follow the same dispute policy.
- Adjudicators (dispute resolvers) should be empowered to set aside overreaching contract provisions. "Overreaching" must be carefully defined but, for example, the agreement that "anyone with a trademark registration wins" is an example of overreaching.
- Domain name holders (but not holders of e-mail addresses) must be known; anonymity is not permitted.
- Some guidance should be provided on jurisdictional issues.